



Title of thesis

**A Novel Seed Based Random Interleaving for OFDM System  
and Its PHY Layer Security Implications**

I, MUHAMMAD ASIF KHAN

allow my thesis to be placed at the Information Resource Center (IRC) of Universiti Teknologi PETRONAS (UTP) with the following conditions:

1. The thesis becomes the property of UTP.
2. The IRC of UTP may make copies of the thesis for academic purposes only.
3. This thesis is classified as

☐

Confidential

☒

Non-confidential

If this thesis is confidential, please state the reason:

---

---

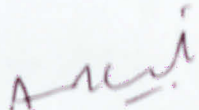
The contents of the thesis will remain confidential for \_\_\_\_\_ years.

Remarks on disclosure:


---

---

Endorsed by



Signature of Author



Signature of Supervisor

Permanent: A- 81 Gulistan Colony Wah Cantt  
Address District: Rawalpindi, Prov: Punjab  
Pakistan

Name of Supervisor  
Assoc. Prof. Dr. Varun Jeoti

Date: 26<sup>th</sup> July 2009

Date: 27<sup>th</sup> July 2009



UNIVERSITI TEKNOLOGI PETRONAS

Approval by Supervisor

The undersigned certify that they have read, and recommend to The Postgraduate Studies

Programme for acceptance, a thesis entitled

**A Novel Seed Based Random Interleaving for OFDM System  
and Its PHY Layer Security Implications**

submitted by

**Muhammad Asif Khan**

for the fulfilment of the requirements for the degree of

**Masters of Science in Electrical and Electronic Engineering**

27<sup>th</sup> July 2009  
Date

Signature

:

Varun Jeoti

Main Supervisor

:

Assoc. Prof. Dr. Varun Jeoti

Date

:

29<sup>th</sup> July 2009

Co-Supervisor

:

\_\_\_\_\_

UNIVERSITI TEKNOLOGI PETRONAS

**A Novel Seed Based Random Interleaving for OFDM System**  
**and Its PHY Layer Security Implications**

By

Muhammad Asif Khan

A THESIS

SUBMITTED TO THE POSTGRADUATE STUDIES PROGRAMME  
AS A REQUIREMENT FOR THE  
DEGREE OF MASTERS OF SCIENCE IN ELECTRICAL AND ELECTRONIC  
ENGINEERING

Electrical and Electronic Engineering

BANDAR SERI ISKANDAR,  
PERAK

July, 2009

## DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTP or other institutions.

Signature: \_\_\_\_\_



Name : Muhammad Asif Khan

Date : 26<sup>th</sup> July 2009



## ACKNOWLEDGEMENT

All praises be to Allah, the most gracious and most merciful, who provided me the courage and strength that enabled me to complete this work. I pray to Him to include me among those who are rewarded for just seeking knowledge.

I would like to express my gratitude and thanks to everyone who encouraged and helped me throughout this research work.

I would like to acknowledge the immense contributions, guidance and encouragement from my supervisor Dr. Varun Jeoti. He has been a mentor and also a friend to me. Throughout the whole duration of this work, I have learnt much from him, not only in terms of technical knowledge but also the finer points of being a better researcher. Without his guidance, this work would not have yielded such positive results and publications at international level. Indeed his dedication is such that it surpasses boundaries of office hours as evident by the hours of personal time that he has spent with me in discussions of the research work.

I would also like to thank my friend Muhammad Asim Khan for his helpful discussions and comments on my work. He was very helpful in answering many of the questions that I had concerning some aspects of the research work. I extend my gratitude to fellow postgraduate and undergraduate students at UTP for their friendship.

I thank my friends Khurram, Raja, Imran, Aamir, Rafi, Mansoor, Rizwan, Mr and Mrs Ayyaz Muhammad and particularly Shahid for their continuous support during my pursuit of this Master Degree.

I would also like to acknowledge the support of Post Graduate office and Electrical and Electronics Engineering Department staff at Universiti Teknologi PETRONAS, MALAYSIA.

I would like express my deepest gratitude and admiration to my parents, whose love, teaching and encouragement enabled me to pursue higher education. I would like to say my sincere thanks to my eldest brother Dr. Qasim Ali Khan, from whom I got inspirations not only in academic education but also in each and every step in my life. He guides me throughout my life for bright future and to become a better person. I would also like to thank my beloved brothers Hashim Ali Khan and Asim Ali Khan; they motivated and guided me to take fruitful decisions for my future. I would also like to thank my beloved sisters for their never ending love who always pray for my success.

*Sincerely*

MUHAMMAD ASIF KHAN

*Dedicated to my beloved Parents,  
Brothers and Sisters*



## ABSTRACT

Wireless channels are characterized by multipath and fading that can often cause long burst of errors. Even though, to date, many very sophisticated error correcting codes have been designed, yet none can handle long burst of errors efficiently. An interleaver, a device that distributes a burst of errors, possibly caused by a deep fade, and makes them appear as simple random errors, therefore, proves to a very useful technique when used in conjunction with an efficient error correcting code.

In this work, a novel near optimal seed based random interleaver is designed. An optimal interleaver scatters a given burst of errors uniformly over a fixed block of data - a property that is measured by so called 'spread'. The design makes use of a unique seed based pseudo-random sequence generator or logistic map based chaotic sequence generator to scramble the given block of data. Since the proposed design is based on a seed based scrambler, the nature of input is irrelevant. Therefore, the proposed interleaver can interleave either the bits or the symbols or the packets or even the frames. Accordingly, in this work, we analyze the suitability of interleaver when introduced before or after the modulation in single carrier communication systems and show that interleaving the bits before modulation or interleaving the symbols after modulation has same advantage. We further show that, in an orthogonal frequency division multiplexing (OFDM) systems, the position of interleaver, whether before or after constellation mapper, has no significance, and is interchangeable. However, scrambling symbols is computationally less expensive than scrambling bits.

For the purpose of analyzing the performance of the proposed seed based random interleaver, simulations are carried out in MATLAB<sup>®</sup>. Results show that our proposed seed based random interleaver has near optimal properties of 'spread' and 'dispersion'. Furthermore, the proposed interleaver is evaluated in terms of bit error rate (BER) versus length of burst error in a single carrier system both before and after modulation. The proposed interleaver out-performs the built in RANDINTLV in MATLAB<sup>®</sup> when used in the same system. It shows that proposed interleaver can convert greater amount of burst errors into simple random errors than that of MATLAB<sup>®</sup> interleaver. The proposed interleaver is also tested in IEEE 802.16e based WiMAX system with Stanford-

University Interim (SUI) channels to compare the performance of average BER versus SNR for both pre modulation and post modulation interleaver. Results show that pre modulation interleaver and post modulation has same performance.

There is also a side advantage of this seed based interleaver, in that it generates a variety of unique random-looking interleaving sequences. Only a receiver that has the knowledge of the input seed can generate this sequence and no one else. If the interleaving patterns are kept secure then it can possibly be used to introduce an extra layer of security at physical (PHY) layer. In that way, at PHY layer, one builds an additional entry barrier to break through and it comes with no extra cost. This property has been investigated by carrying out key sensitivity analysis to show that the attacks to guess key can be very futile, as difference at 4<sup>th</sup> decimal place in the initial condition can lead to entirely different scrambling.



<b>List of Figure.....</b>	<b>xiii</b>
<b>List of Tables.....</b>	<b>xiv</b>
<b>List of Abbreviations .....</b>	<b>xv</b>
 <b>CHAPTER 1: INTRODUCTION.....</b>	 <b>01</b>
1.1 Motivation.....	01
1.2 Typical Wireless Communication System.....	03
1.3 Interleaver.....	04
1.3.1 Importance of Interleaver.....	05
1.4 Research Objectives .....	06
1.4.1 Design of Seed Based Random Interleaver.....	06
1.4.2 Comparison of Pre- Modulation vs. Post Modulation Interleaver.....	06
1.4.3 Interleaving in OFDM system .....	06
1.4.4 Study of PHY Layer Security Aspects of Proposed SBR Interleaver....	07
1.5 Scope of the Proposed Work.....	07
1.6 Thesis Contribution .....	08
1.7 Organization of Thesis.....	09
 <b>CHAPTER 2: BACKGROUND &amp; LITERATURE REVIEW.....</b>	 <b>11</b>
2.1 Wireless Channels.....	12
2.2 Typical Wireless communication System.....	16
2.3 Interleavers.....	17
2.3.1 Types of Interleaver.....	17
2.3.1.1 Non- Random Interleavers.....	17
2.3.1.2 Random Interleaver.....	18
2.3.1.3 Algebraic Interleaver.....	19
2.3.2 Random Interleavers and Literature Review.....	20
2.3.2.1 Random Interleaver Properties.....	21
2.3.2.2 Literature Review.....	23



2.4	Security Implications.....	29
2.5	Wireless Security Preliminaries and Related Literature Review.....	30
2.5.1	Typical Model of Security.....	31
2.5.2	Security Requirement.....	33
2.5.2.1	Basic Security Mechanisms.....	33
2.5.2.2	Wired Vs. Wireless .....	34
2.5.3	Security Threats.....	35
2.5.4	Related Literature Review on Wireless Security.....	40
2.5.5	Interleaver as PHY Layer Security Device .....	45
2.5.6	PHY Layer Security .....	46
2.6	Summary.....	48

### **CHAPTER 3: NOVEL SEED BASED RANDOM INTERLEAVER WITH IMPROVED PERFORMANCE: DESIGN AND ANALYSIS....**

3.1	Objectives.....	51
3.2	Performance Parameters of Seed Based Random Interleaver.....	53
3.2.1	Spread.....	53
3.2.2	Dispersion.....	53
3.2.3	BER as a Function of Length of Burst Errors.....	53
3.3	Design of Proposed Interleaver - Seed Based Random Scrambling (SBRS)....	54
3.3.1	Scrambling Based Interleaver.....	55
3.3.2	Seed Based Random Scrambler- The Algorithm.....	57
3.3.3	Initialization of SBRS.....	60
3.3.3.1	Extracting unique initial condition from external key.....	60
3.3.4	Scrambling Algorithm.....	61
3.3.5	Descrambling Algorithm.....	64
3.4	Performance Parameter Analysis- Spread and Dispersion.....	64
3.4.1	Simulation Model Parameter for Spread and Dispersion.....	64
3.4.2	Results and Analysis.....	66
3.4.2.1	Analysis of SBR Interleaver Spread.....	66

3.4.2.2	Analysis of SBR Interleaver Dispersion.....	75
3.5	Performance Parameter Analysis- BER as a Function of Length of Burst Error.	79
3.5.1	Comparison of SBR Interleaver with Random Interleaver.....	79
3.5.2	Introduction of SBR Interleaver in Conventional Communication System.....	82
3.5.2.1	Proposed Post Modulation Interleaver.....	82
3.5.2.2	Comparison of Pre- modulation and Post Modulation Interleaver.....	82
3.5.3	Introduction of SBR Interleaver in OFDM System- Before and After Constellation Mapper.....	85
3.6	Summary.....	93
<b>CHAPTER 4: SBR INTERLEAVER AS A PHY LAYER SECURITY DEVICE.....</b>		<b>95</b>
4.1	Introduction.....	96
4.2	Performance parameter- Key Sensitivity Analysis.....	97
4.2.1	Positional Significance of Each Character in the External Key.....	103
4.3	Effectiveness of SBR Interleaver as a Security Device.....	105
4.3.1	Traffic Analysis/ Passive Eavesdropping .....	105
4.3.2	Data Forgery Attacks .....	107
4.3.3	Denial of Service Attack .....	107
4.4	Summary .....	108
<b>CHAPTER 5: CONCLUSION.....</b>		<b>109</b>
5.1	Conclusion.....	109
5.2	Contribution of the Work.....	111
5.3	Suggested Future Work.....	112



## List of Figures

Figure 1.1: Block Diagram of Typical Wireless Communication System.....	04
Figure 2.1: Types of fading.....	13
Figure 2.2: Channel quality variation with time scales.....	14
Figure 2.3: Multipath propagation.....	15
Figure 2.4: Typical model of encryption and decryption.....	31
Figure 3.1: Block diagram of seed based scrambler design.....	56
Figure 3.2: Achieved Spread of SBR Interleaver with $S < 2$ and $S < 3$ .....	66
Figure 3.3: Histogram of SBR Interleaver Spread Pairs.....	67
Figure 3.4: Histogram of low probability to generate spread $S < 2$ .....	67
Figure 3.5: SBR Interleaver Dispersion with $N= 64,128$ and $256$ .....	78
Figure 3.6: Histogram of SBR Interleaver Dispersion.....	78
Figure 3.7: Burst Error Comparison of Proposed SBR Interleaver with Random Interleaver for 8-PSK and $N=512$ .....	81
Figure 3.8: Block Diagram of Proposed Pre- modulation SBR Interleaver.....	83
Figure 3.9: Block Diagram of Proposed SBR Post Modulation Interleaver.....	84
Figure3.10:Comparison of proposed pre- modulation and post modulation Interleaver with 8-PSK.....	85
Figure3.11:Block Diagram of Proposed OFDM System with SBR Pre- and Post Modulation Interleaver.....	87
Figure3.12:Pre- modulation Interleaver Performance for QPSK with RS-CC $\frac{1}{2}$ and SUI 1, 3, 5.....	91
Figure3.13:Post- modulation Interleaver Performance for QPSK with RS-CC $\frac{1}{2}$ and SUI 1, 3, 5.....	92
Figure 4.1: Block diagram of proposed SBR Interleaver as a PHY layer security device for OFDM system.....	97
Figure 4.2: Probability of occurrence of constellation points with slightly different initial condition.....	99



## List of Tables

Table 3.1(a): Chaotic SBR Spread with $N=128$ and Spread $\leq 2$ .....	69
Table 3.1(b): RAND Based SBR Spread with $N=128$ and Spread $\leq 2$ .....	70
Table 3.2(a): Chaotic SBR Spread with $N=256$ and Spread $\leq 3$ .....	71
Table 3.2(b): RAND Based SBR Spread with $N=256$ and Spread $\leq 3$ .....	72
Table 3.3(a): Chaotic SBR Interleaver Spread with $N=512$ and Spread $\leq 4$ .....	73
Table 3.3(b): RAND Based SBR Interleaver Spread with $N=512$ and Spread $\leq 4$ .....	74
Table 3.4(a): SBR Dispersion with $N=64, 128, 256$ with Chaotic Input Seeds.....	76
Table 3.4(b): SBR Dispersion with $N=64, 128, 256$ with Rand Function.....	77
Table 3.5: Specifications of 6 Burst Profiles.....	88
Table 3.6: Number of Coded Bits per OFDM Symbol.....	89
Table 3.7: Terrain Type and Corresponding Sui Channels.....	89
Table 3.8: General Characteristics of SUI Channels.....	89
Table 4.1: Probability of Wrong Input Elements with Different Key using Chaotic Sequence.....	100
Table 4.2: Probability of Wrong Input Element with Different Key using RAND function.....	100
Table 4.3: Position Vector Generation with Slight Change in Initial Condition.....	101
Table 4.4: ICs for Typical External Secret Keys.....	104

## LIST OF ABBREVIATIONS

AES	Advance Encryption Standard
AP	Access Point
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CCMP	Counter mode/CBC MAC Protocol
CD	Compact Disc
CK	Canetti-Krawczyk
CLM	Chaotic Logistic Map
CRC	Cyclic Redundancy Check
DoS	Denials of Service
DS/SS	Direct Sequence/Spread Spectrum
EAP	Extensible Authentication Protocol
FBWA	Fixed Broadband Wireless Access
FEC	Forward Error Correction
FFT	Fast Fourier Transform
HSDP	Hierarchical Data Security Protocol
ICV	Integrity Checksum Value
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
ISI	Inter Symbol Interference
IV	Initialization Vector
LAN	Local Area Network
LOS	Line-Of-Sight
MIC	Master Initial Condition
MitM	Man-in-the-Middle
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NIC	Network Interface Card

OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PHY	Physical
PS <sub>k</sub> K	Pre-Shared Key
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RC4	Rivest Cipher 4
RNG	Random Number Generator
RSGF	Random Sequence Generator Function
RSNA	Robust Security Network Association
RTS	Request to Send
SBR	Seed Based Random
SBRS	Seed Based Random Scrambling
SISO	Single Input Single Output
SK	Session Key
SNR	Signal-to-Noise Ratio
SSID	Service Set Identifier
SUI	Stanford University Interim
TKIP	Temporal Key Integrity Protocol
UM	Unauthenticated-link Adversarial Model
VoIP	Voice over IP
WEP	Wired Equivalence Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access



## Chapter

# 1

## Introduction

### 1.1 Motivation

Given the tremendous benefits a wireless technology brings along, most networks, local or otherwise, are not only adopting it but also evolving with it. The wireless technology offers, among others, lower cost, easier installation and mobility – a flexibility that no fixed network can offer. For example, a wireless local area network (WLAN) is not physically connected as wired LANs are and it works through the air. Consequently, it is expected that the reliability of data is doubtful due to error prone nature of wireless channels caused by fading and multipath. The utmost goal for reliable data transmission is that the received data are as close as possible to the transmitted data themselves. Hence, various techniques have been developed to deal with and help to improve the reliability of data over wireless channels. Among them, an interleaver is considered to be an efficient and fairly simple technique that easily improves the reliability of a wireless network. An interleaver distributes a burst of errors, possibly caused by a deep fade, and makes them appear as simple random errors. When it is employed together with channel coding techniques, the burst of errors are converted into simple random errors by the

interleaver and are then corrected by the channel codes. An interleaver could be designed both as a random interleaver or a non-random interleaver. A random interleaver which is dependent on a unique seed could be used as a physical (PHY) layer security device to scramble the data randomly. In that way, at PHY layer, one builds an additional entry barrier to break through and it comes with no extra cost.

The motivation of this thesis is to design a seed based random interleaver having optimal interleaving properties. An optimal interleaver must scatter a given burst of errors uniformly over a fixed block of data - a property that is measured by so called 'spread'. How randomly does an interleaver spread the given burst of errors every time is, however, measured by what is called 'dispersion'. In this thesis, the idea is to use a pseudo-random sequence generator or logistic map based chaotic sequence generator together with a unique seed and thereby design a unique scrambling matrix. The proposed scrambler in the interleaver gives rise to very good spread and dispersion. Since our design is based on a seed based scrambler, the nature of input is irrelevant. Therefore, our interleaver can interleave either the bits or the symbols or the packets or even the frames. Accordingly, the motivation is to also show that interleaving the bits before modulation or interleaving the symbols after modulation has the same advantage. However, interleaving post-modulation symbols requires smaller scrambling matrix size for  $M$ -ary modulations as compared to that that interleaves bits.

There is also a side advantage of this seed based interleaver, in that it generates a variety of unique random-looking interleaving sequences. Only a receiver that has the knowledge of the input seed can generate this sequence and no one else. If the interleaving patterns are kept secure then it can possibly be used to introduce an extra layer of security at physical (PHY) layer. An added motivation is to analyze the security implications of the proposed interleaver.



## 1.2 Typical Wireless Communication System

A tremendous increase in the demand for information exchange is a unique characteristic of modern internet based development. The transfer of information from source to its destination should be done in such a way that the quality of received information should be as close as transmitted information. A typical block diagram of wireless communication system is shown in Figure 1.1. It illustrates the signal flow through a typical wireless communication system. The upper blocks constituting a transmitter show an information source block, a source encode block, an encryption block, a channel coding block, an interleaver block and a modulation block. The lower blocks indicate the signal transformation from receiver to sink or received sourced information. The lower blocks essentially reverse the signal processing steps formed by the upper blocks. During the last two decades, other signals processing functions have been frequently incorporated within the same assembly as the *modulator* and *demodulator*, together called *modem*.

The information to be transmitted, such as images, voice or speech, computer data etc., is machine formatted regardless of its source. Formatting the source information makes it compatible with the signal processing within a communication system. *Source encoding* step produce analog- to- digital conversion and removes the redundant information. In order to ensure the secrecy of transmitted information, an *encryption* scheme must be used. The data must be protected against perturbation introduced by wireless channels, which could lead to misinterpretation of transmitted information at receiver. *Channel coding* can reduce the probability of error introduced by the channels at the expense of bandwidth or decoding complexity. In order to further improve the performance of the channel coding and allow it to use not-so-complex error-correcting codes in burst noise caused by deep fades, *interleaving* is introduced. Interleaver will be discussed in details in the following section. *Modulation* is then used to convert the data to certain waveforms that can be transmitted over the wireless channel.



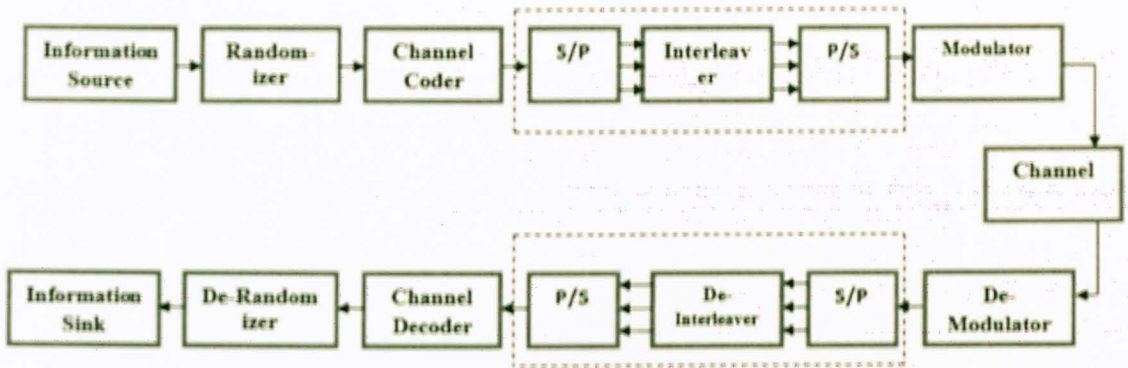


Figure 1.1: Block Diagram of Typical Wireless Communication System

### 1.3 Interleaver

As mentioned before, interleaving is a process of rearranging the positions of input data elements in a given data block. In other words, an interleaver simply makes the permuted sequence of input data elements. Associated with any interleaver is a de-interleaver that restores the original sequence. In order to obtain correct sequence at the receiver side, same interleaving pattern should be used by the de-interleaver.

An interleaver, generally used after channel coding so as to rearrange the ordering of coded data (refer to Figure 1.1). Therefore, the presence of interleaver after channel coding, to a great extent, mitigates the problem of the transmitted data that are corrupted with burst errors. The burst errors corrupt contiguous data elements of input sequence of data and make it infeasible to detect and correct them at receiver side. Thus, an interleaver in between channel coding and modulation helps to disperse the neighboring data elements.

Wireless channels having memory exhibit mutually dependent errors. Under the assumption that the channel has memory, the errors no longer can be characterized as randomly distributed single bit errors. Instead it occurs in bursts, corresponding to the time when the channel is in deep fades. Interleaving the coded bits before transmission spreads out the burst of channel errors in time in such a way that it appears as random

errors at the decoder – easily handled by the decoder. The presence of interleaver after coded bits drastically improves the performance of channel coding [A. Goldsmith et al 2005]. The following subsection summarizes the importance of interleaver design for wireless communication system.

### 1.3.1 Importance of Interleaver

Interleaver has emerged as a simple and an efficient technique that immensely improves the performance of communication system in burst errors. Interleaver plays an important role in minimizing the probability of errors in fading channel. Interleaver decorrelates the adjacent coded bits in time such that the burst errors appear at demodulator as random but simple errors. Channel coding techniques like block codes [P. Elise et. al. 1954], concatenation codes [G. D. Forney et. al. 1966] and multi-level codes [H. Imai et al. 1977] are designed to detect and correct a specific number of random errors depending on the error detecting and correcting capability of the given code. The block and convolutional codes are designed to work well with additive white Gaussian noise (AWGN) channels. The performance of random error-correcting codes are worse in fading channels because they cannot handle the long burst of errors introduced due to deep fades in fading channels. Moreover, the burst errors correcting codes are complex and so are computationally expensive to correct the long burst of errors. Hence, in order to make it possible to use simple random error-correcting codes, an interleaver is employed after channel coding. In other words, interleaver converts memory channel into memoryless channel and renders burst errors as simple random errors that are easily corrected by conventional error-correcting codes.

Interleaver facilitates and improves the design of wireless communication system at many layers of OSI (Open System Interconnection) model. To ensure reliability at MAC layer, coding is combined with interleaving. Most importantly, interleaver plays a key role and improves the performance of turbo codes significantly. A lot of work has been done in this field to design and analyze the interleaver for turbo codes. Interleaver also has been employed at transport layer to analyze the performance of interleaver to detect and correct burst errors in speech recognition. To improve the performance of video and



multimedia application in fading channel at higher layer, interleaver also plays an important role in minimizing the burst noise.

## **1.4 Research Objectives**

There are four main objectives of this research work. These are outlined as follows:

### **1.4.1 Design of Seed Based Random Interleaver**

First objective of this thesis is to design a novel seed based random interleaver to obtain near optimal performance in burst like environment. In order to introduce randomness in design, random sequence is generated using two techniques, namely the MATLAB RAND function that is dependent on pseudo-random numbers and also chaos using well known chaotic logistic map (CLM). The design objective of random interleaver is that it should have good inherent random interleaving properties. These properties need to be evaluated to learn whether CLM based design or RAND function design is superior or none.

### **1.4.2 Comparison of Pre- modulation vs. Post Modulation Interleaver**

Secondly, wireless communication system design will be further explored by changing the position of interleaver. The bit level interleaver, also called pre- modulation interleaver herein, will be compared with symbol level interleaver, called post modulation interleaver. It is observed that the interleaving operation can be commutated with modulation without loss of performance.

### **1.4.3 Interleaving in OFDM Systems**

Next, the suitability of seed based interleaver design for OFDM system will be experimented. The performance of seed based random interleaver will be analyzed both at bit level and symbol level. At bit level seed based interleaver will replace already used block interleaver, and at symbol level seed based interleaver introduces after modulation to scramble the OFDM constellation symbol. It is observed that seed based interleaver will perform the same at both pre- modulation and at post modulation.



#### 1.4.4 Study of PHY Layer Security Aspects of Proposed SBR Interleaver

Finally, since the seed based random interleaver scrambles the symbols at physical (PHY) layer, the suitability of this mechanism is also studied as a PHY layer security device. The interleaver design will be analyzed for possible wireless threats. Moreover, the suitability of interleaver at post modulation will also be analyzed and compared with pre-modulation to ensure the security benefits at PHY layer with modified system.

#### 1.5 Scope of The Proposed Work

- A seed based random interleaver is designed and simulated in MATLAB® so as to evaluate its performance. Random interleavers, in general, are evaluated based on their properties of spread and dispersion. The random interleaving properties of proposed design are analyzed using two random sequences: chaotic sequence based on chaotic logistic map and MATLAB® RAND function based on pseudo-random sequence. The study includes evaluation of their respective performance in terms of their properties of spread and dispersion. The proposed SBR Interleaver is compared with MATLAB® random interleaver in burst error environment and burst of errors are introduced manually.
- The study of post modulation interleaver is also reported in the thesis. The position of interleaver after channel coding in typical communication system has been changed and introduced after the modulation. A typical communication system is developed in MATLAB® so as to facilitate the comparison of pre and post modulation SBR Interleaver.
- Furthermore, as mentioned before, the proposed interleaver is also used in an OFDM system. The performance results of pre and post constellation mapper interleaver are obtained for an OFDM based worldwide interoperability for microwave access (WiMAX) system. At the end, a complete end-to-end IEEE 802.16d compliant fixed broadband wireless access (FBWA) system, an early model of WiMAX system, is developed in MATLAB-SIMULINK.

- The seed based design of random interleaver can generate different interleaving patterns by changing input seed. At PHY layer, proposed seed based random interleaver can be employed as security device where seeding parameter works as a key. In order to evaluate proposed seed based random interleaver design against brute force attack and various data forgery attack, key sensitivity analyses are considered, analyzed and reported.

## 1.6 Thesis Contributions

- In this research, a novel design of seed based random interleaver is reported. To evaluate performance, proposed scheme is initialized with two random sequences: chaotic sequence using chaotic logistic map and MATLAB RAND function. Previously, randomly generated interleavers have tradeoff based on their complexity and performance. As a result, the performance of interleaver for specific application can be optimized by paying the price of complexity with increased memory requirement. In this work, as an alternative, we proposed seed based random interleaver. The proposed interleaver is shown to have good interleaving properties measured in terms of spread and dispersion.
- It is also shown that the spread and dispersion of both CLM based SBR Interleaver and RAND based SBR Interleaver are quite same.
- This thesis also analyzes the performance of interleaver when it is deployed either pre- or post modulation stage. The comparison of pre- and post modulation interleaver is carried out in terms of complexity and interleaving performance like dispersion and spread. Interleaver performance remains same at both pre- and post modulation position, but complexity of interleaving is minimized for post modulation.
- The proposed scheme is analyzed, for burst error correction capability, and compared with MATLAB random interleaver. Our proposed design efficiently converts larger number of burst errors into simple errors as compared to MATLAB random interleaver.



- The proposed interleaver is also analyzed in an OFDM system. A WiMAX model compliant with IEEE802.16d is developed and the interleaver block is introduced at both pre- and post constellation mapper block. The performance of the said interleaver is compared. The performance of proposed Interleaver at both locations is same.
- Finally, proposed seed based random interleaver is exploited as a PHY layer security device. The seeding parameter is used as the unique key. Accordingly, it should have enough key space to avoid attacks. In order to analyze the effectiveness of proposed technique at lowest layer, likely capabilities of attacks, such as brute force and data forgery attacks, against proposed scheme are analyzed. The key-sensitivity is carried out to evaluate the performance against brute force and various data forgery attacks.
- Furthermore, security mechanisms in practice are scrutinized in detail to uncover the wireless security threats that are still possible due to unprotected PHY layer data, such as coding, interleaving and modulation pattern, clients address and management & control information. Based on said analysis, countermeasures are proposed at PHY layer to increase the entry barrier to break in.

## 1.7 Organization of Thesis

This work is structured as follows:

- Chapter 1 has focused on presenting the motivation, summary, background, objectives, scope and specific contributions of the work.
- Chapter 2 is about background and literature review. It first presents the types of errors introduced by the wireless channel. It is followed by literature review of various types of random interleavers that have been developed by researchers. This is to show that there is a need for seed based random interleaver design that has better interleaving properties and has simpler structure for flexibility.



- Chapter 3 presents the design and analysis of proposed seed based random interleaver. Seed Based Random Scrambler is designed where random input sequence is generated using two different generators based on chaos using well-known chaotic logistic map and MATLAB RAND function. The proposed design retains the randomness in design by avoiding the repetition of random numbers generated using said methods. The output range  $[0.1, 0.9]$  divided into equal sub-intervals of size equal to interleaver length to design. The unique property of our design is to avoid any repetition within these sub-intervals to design a unique scrambling matrix. In order to interleave each block using different scrambling matrix, extraction of new seed/ initial condition is also discussed in this chapter.

This chapter also presents the simulation parameters to obtain results and to measure the performance of seed based random interleaver. It lists the selected parameter for proposed wireless transmission systems and OFDM based system i.e. pre- and post modulation interleaver to compare the performance of proposed interleaver with random interleaver in burst errors environment. The comparison of pre- and post modulation interleaver in term of complexity and performance is analyzed. Results show that proposed scheme has good random interleaving properties and do not dependent of random sequences used to generate interleaving patterns. Moreover, changing the position to post modulation interleaving has no effect on the performance of the system. Further, interleaving complexity can be minimized with post modulation interleaving.

- Chapter 4 discusses the suitability of proposed seed based random interleaver as a PHY layer security device. In order to analyze the PHY layer security aspects of proposed technique, key sensitivity analysis are carried out. Moreover, various security attacks are discussed in terms of proposed system to analyze its effectiveness as a PHY layer security device.
- Finally, the conclusion of entire work is given in chapter 5.

## Chapter

# 2

## Background & Literature Review

The chapter 1 focused on the motivation, objective, scope and the contribution of research. It gave an overview of typical wireless communication model to highlight the various wireless communication system building blocks.

This chapter presents and analyzes the literature available on interleaver and suggests how to improve the performance of wireless communication system in wireless channels with burst errors. In this chapter, the overview of wireless channel is presented first. It is followed by, the comparison of various types of interleavers and also the related literature review on random interleavers in terms of design, properties, complexity in interleaving and applications.

Furthermore, this chapter also focuses on the suitability of interleaver as PHY layer security device. The preliminary concepts and mechanisms of wireless network are discussed first to familiarize with the concepts. The security threats on wireless network to pin point the security weaknesses of wireless network are given next. The related literature review on wireless security to suggest the security improvement and countermeasures is discussed towards the end.



## 2.1 Wireless Channels

Before going into detail discussion of random interleaver and its literature review, let us introduce the wireless channels. A defining characteristic of the mobile wireless channel is the variations of the channel strength with time and frequency. The variations can be roughly divided into two types "Large- scale fading and Small- scale fading". Large-scale fading occurred due to path loss of signal as a function of distance and shadowing by large objects such as building and hills. This occurs as the mobile user moves through the distance of the order of the cell, and is typically frequency independent. Small- scale fading occurs due to constructive and destructive interference of multipath signals paths between the transmitter and receiver. It is at the spatial scales of the order of the carrier wavelength, and is typically frequency dependent. In other words, small- scale fading or simply fading is used to describe the rapid fluctuations of the amplitude, phase or multipath delays of a radio signal over a short period of time or travel distance, so that large scale- path loss effects may be ignored. Fading is caused by interference between two or more version of the transmitted signal which arrives at the receiver at slightly different time. These waves, called multipath waves, combine at the receiver antenna to a resultant signal which can vary widely in amplitude and phase, depending on the distribution of the intensity and relative propagation time of the waves and the bandwidth of the transmitted signal. Fading has two independent mechanisms: Time dispersion (due to multipath delays) and Doppler spread (due to motion of the mobile or channel). Figure 2.1 summarize the fading due to delay spread and Doppler spread. Fading due to Doppler spread causes two degradations, slow fading and fast fading. Slow fading causes the deep fades that will affect many simultaneous bits/symbols in error. These introduced errors lead to disruption in transmitted signal. Thus, slow fading may lead to large burst of errors and information data within such interval completely lost, which cannot be corrected with simple single error correcting techniques. Therefore, these burst errors can seriously degrade the performance of wireless communication system.



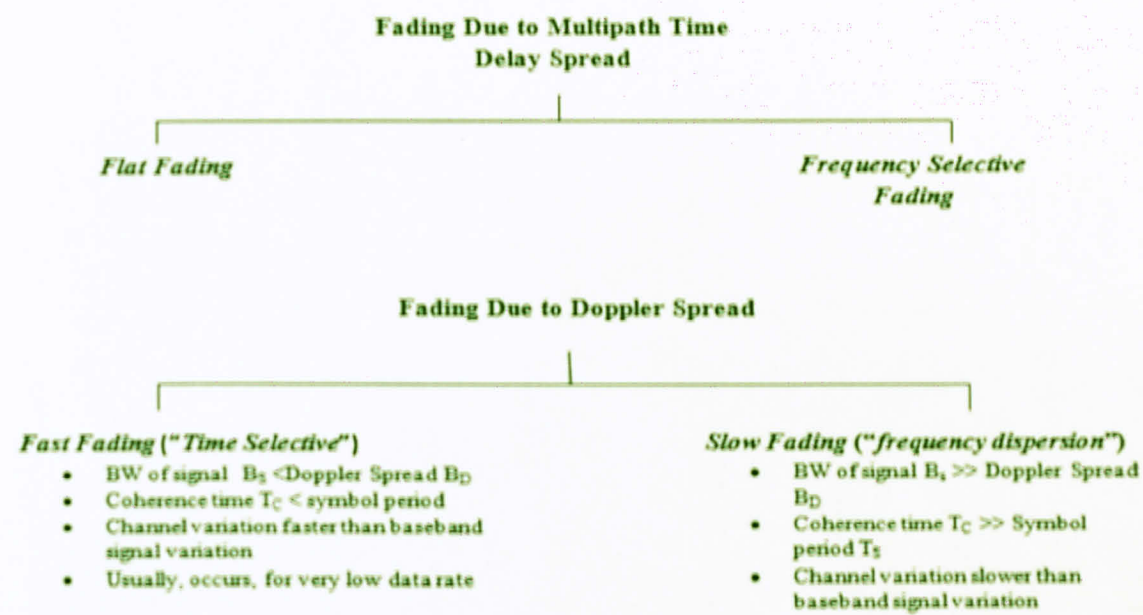


Figure 2.1: Types of fading

A wireless channel generally referred to as introducing slow fading, if channel coherence time is sufficiently large as compared to symbols time. In other words, the time duration that the channel behaves in a correlated manner is long compared with the time duration of a transmitted symbol. The long burst of errors also introduced, if channel varies slower as compared to baseband signal and it disrupts large part of information signal into deep fades and information within such interval is lost. Channel quality varies over multiple time-scales as shown in Figure 2.2.

The wireless channel is the single most important factor that limits the performance of wireless communication system. It is extremely hostile to communication. The transmission path between the transmission and the receiver can vary from simple Line of Sight (LoS) to one that is severely obstructed by building, mountain and foliage. Unlike wired channels that are stationary and predictable, radio channels are extremely random and do not offer easy analysis. The signal from the transmitter is reflected, diffracted and

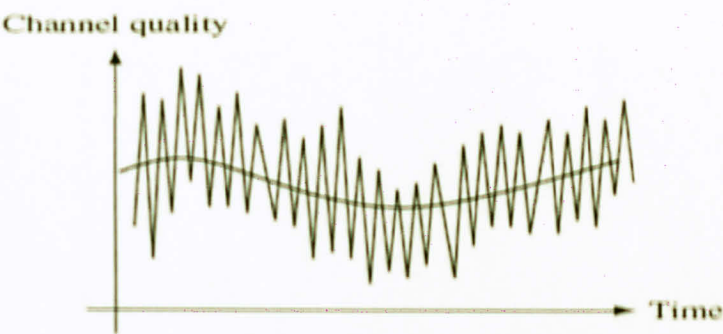


Figure 2.2: Channel quality variation with time scales

scattered by various objects in the surrounding before reaching the receiver. When the signal impinges on an object that is very large compared to its wavelength, it will be reflected. Example of reflecting objects are the earth’s surface, building and walls. On the other hand, diffraction happens when the signal seemingly bends around obstacle that obstructs the path between the transmitter and receiver. When the signal impinges on objects that are small compared to its wavelength, scattering occurs.

The three signal propagation mechanisms (reflection, diffraction and scattering) affect the received signal strength. Naturally, the signal strength will be lower the farther the receiver is from the transmitter due to the spread of the signal in all direction through free space. Making matters worse, a signal from the transmitter can take multiple different paths before reaching the receiver. This can be caused by reflecting or even scattering objects. The multiple reflected versions of the signal will arrive at the receiver at slightly different time and with various amplitudes and phases. This phenomenon is called multipath. The multipath signals add up vectorially. The received signal strength will be amplified if the signals reinforce each other or are in phase with one another. The received signal strength can also drop drastically to a level that impedes any communication if the signals cancel each other or are out of phase. This is also known as multipath fading and is detrimental to wireless communications.

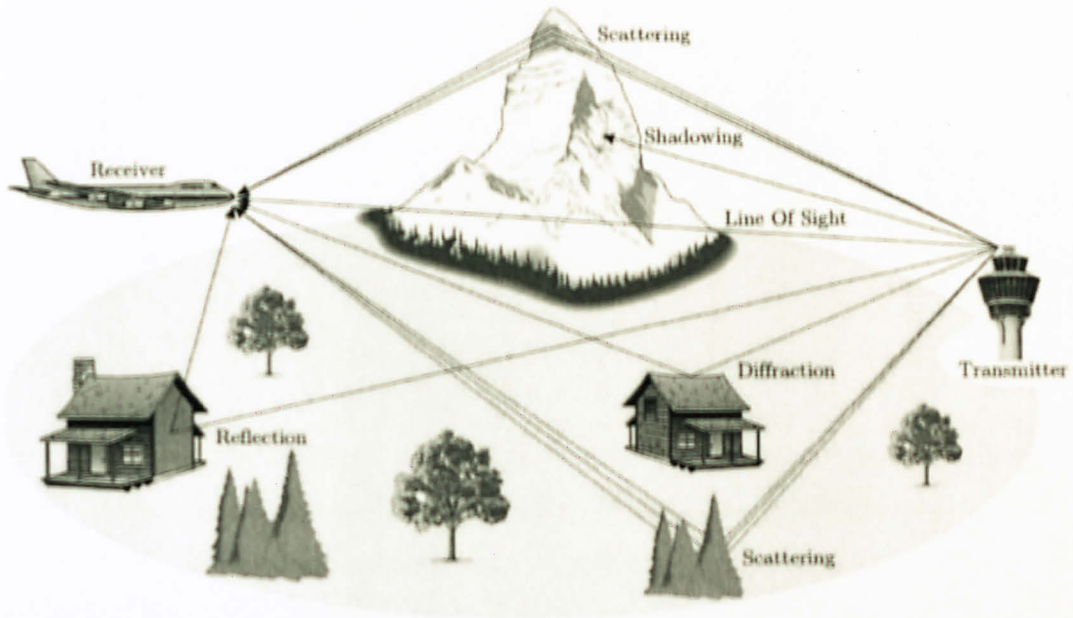


Figure 2.3: Multipath propagation  
(Referenced from the website: [www.cs.nccu.edu.tw](http://www.cs.nccu.edu.tw))

Multipath in the radio channel creates small- scale fading effects. The three most important effects are:

- Rapid change in the signal strength over a small travel distance or time interval
- Random frequency modulation due to Doppler shifts on different multipath signals
- Time dispersion (echoes) caused by multipath propagation delay

In buildup urban areas, fading occurs because the height of the antennas is well below the height of the surrounding structure, so there is no single LoS path to the base station. When LoS exists, multipath still occurs due to reflections from the ground and surrounding structure. The signal arrives from different direction with different propagation delay. The received signal at any point in space may consist of a large





Figure 2.3: Multipath propagation  
(Referenced from the website: [www.cs.nccu.edu.tw](http://www.cs.nccu.edu.tw))

Multipath in the radio channel creates small- scale fading effects. The three most important effects are:

- Rapid change in the signal strength over a small travel distance or time interval
- Random frequency modulation due to Doppler shifts on different multipath signals
- Time dispersion (echoes) caused by multipath propagation delay

In buildup urban areas, fading occurs because the height of the antennas is well below the height of the surrounding structure, so there is no single LoS path to the base station. When LoS exists, multipath still occurs due to reflections from the ground and surrounding structure. The signal arrives from different direction with different propagation delay. The received signal at any point in space may consist of a large

number of plane waves having randomly distributed amplitudes, phases and angles of arrival. These multipath components combine vectorially at the receiver, and can cause received signal to distort or fade. In Wireless LAN the receiver is stationary; the received signal may fade due to movement of surrounding objects in the channel. As a result of Rayleigh fading, error bursts may get introduced at the receiver of the wireless system. So it is highly desirable to design an optimum and suitable Interleaver for such wireless systems to combat burst errors introduced due to fading channel.

## 2.2 Typical Wireless Communication System

In typical wireless communication system interleaver is introduced after channel coding to minimize the effect of wireless channels that causes burst of errors. The deep fades caused by wireless channel disrupts large number of information bits/symbols in error. These errors cannot be corrected with simple error correcting techniques. In order to further improve the performance of channel coding and allow it to use not-so-complex error-correcting codes in burst noise caused by deep fades, *interleaving* is introduced. The block diagram of wireless communication system where interleaver is introduced after channel coding is shown in Figure 1.1 in chapter 1. Interleaver can interleave either bits, symbols, packets or even frame in block by block manner or can take serial data interleave. For block interleavers, conversion from serial to parallel block after channel coder and parallel to serial block after interleaving considered being optional. The functionality of conversion from serial to parallel and parallel to serial is performed within interleaver block. The details of other building blocks of wireless communication system have been discussed in chapter 1.

## 2.3 Interleavers

Interleaver has been used in communication systems to combat burst errors introduced due to fading channel. Interleavers are categorized based on their design methods, complexity, interleaving properties and their suitability for given application. Broadly speaking, interleavers are divided into three main types, namely non- random, random and algebraic interleavers. The comparison and detailed discussion on different types of interleaver is given in later sections. The design of random interleavers is an active research area. The properties of random interleaver help improve the performance and optimally interleave the transmission data. Next subsection presents the random interleaver, its properties and related literature review.

### 2.3.1 Types of Interleaver

Interleaver designs are mostly applications specific. Therefore, design of interleaver should follow and based on some specific factors named as wireless channel condition, complexity of the system and characteristics of application. Hence, introduction of interleaver families that are designed till now are an attempt to give meaningful picture of evolution in design based on increasing demand of reliable information exchange and characterize the modern trends. Interleavers are categorized based on their complexity, efficiency and design criteria. The following section gives a summary of main techniques to design interleaver.

#### 2.3.1.1 Non- Random Interleavers

The basic idea of interleaving is to mix up codeword symbols in such a way that the burst errors that are introduced in wireless transmission of data should spread out across different codewords as much as possible and it appears as single random errors. To achieve this, one class of interleavers are generated with non- random permutation or analytical way such as:



- One simplest method of designing non- random permutation in which codeword symbols are written row- wise and read out column- wise called block interleaver. For example,  $(d, k)$  row and column respectively, codewords are separated by  $d-1$ , so that the symbols in same codeword experience approximately independent fading if their separation in time is greater than the channel coherence time. Block interleaver is commonly used with block codes in a typical wireless communication system.
- Other improved designs based on block interleavers are odd- even and helical interleavers. If block codes have odd number of rows and odd number of columns then it is also called odd- even interleaver. Basically, with this approach the code power is uniformly distributed. An interleaver, in which data is written row wise but the data is read diagonally called helical interleaver.
- Another type of non- random interleaver is circular/ cyclic shift. The basic formula is

$$\pi(j) = (aj + r) \bmod N$$

where  $r < N$  is an offset and  $a < N$  is a step time that is relative to  $N$

In [J. J. Boutros et al. 2005] author improves the design with quasi- cyclic interleaving in term of memory requirement and performance efficiency for turbo codes.

### 2.3.1.2 Random Interleaver

The non- random interleavers discussed earlier are based on limited design objectives to separate the most problematic weight- 2 sequence or try to spread out the adjacent bits. Therefore, it should be easy to improve to some extent the spread or generate sequence with higher weight when the size  $N$  is large without even trying to optimize interleaver. Unfortunately, non- random interleaver break up the low weight sequences but posses a lot of regularity. This regularity perhaps increases the possibility that the non random permutation will reproduce the bad sequences again. To prevent this, one might design an interleaver which simultaneously breaks up all the low weight sequence in an optimal way.

The design of random interleaver to achieve optimal performance is an active research area. Random interleavers are built using random permutations on  $N$  integers, selected at random. An overview of class of random interleaver design to follow non random interleaver design objective with good spread or break up low weight sequences but retaining some degree of randomness is given below:

- Semi random interleaver or also called ' $S$ ' type interleaver originally proposed by [J. L. Ramsey, et al, 1970] and later on, based on same principle semi random interleavers are analyzed for turbo codes and named as semi random interleaver [D. Divsalar et al. 1995]. Therefore, to avoid identical permutation, semi random interleaver is defined as follows: Each randomly selected integer is compared to the  $S$  previously selected integers. If the current selection is equal to any of the  $S$  previous selection within a distance of  $\pm S$  then the current selection is ignored. This process is repeated until all  $N$  integers are selected. The search time for this algorithm is increased with the size  $N$ , and it is not guaranteed that it will finish successfully. However, choosing  $S < \sqrt{N/2}$  usually produce a solution in reasonable time. Therefore, the design of  $S$ - random interleavers are dependent on careful selection of  $S$  parameter and random source that eventually improves the interleaver design. Moreover, if  $S=1$ , the  $S$ - random interleaver reduces to purely random interleaver.

### 2.3.1.3 Algebraic Interleaver

Random interleaver design discussed earlier, significantly improves the performance by avoiding identical permutation and retaining degree of randomness. But, unfortunately, memory requirement is increased with the selection of parameter  $S$  and with the size of interleaver. To deal with memory 'Algebraic Interleavers' are proposed. These interleavers can be generated on- the- fly with fewer design parameters and exhibits reasonable randomness in the interleaver pattern. A short selection of interleavers described by [C. Berrou, et al. 1993][Andrews et al. 1998][Sadjapour, et al. 2001] [C. J. C. Bravo et al. 2003] and relative prime and golden prime interleavers described in [S. N. Crozier, et al. 1999] belongs to this family of interleavers.



Algebraically constructed interleavers are considered to be a good design for memory efficient applications. Furthermore, the design also considered important becomes of analytical ease, simple design with fewer parameters, and efficient for practical hardware implementation.

From all above interleaver design types, this section conclude by considering that, interleaver plays an important role in all applications of transmission system spread over OSI layers. Interleaver is designed to fulfill specific system requirement. Therefore, one should look into the designs of interleaver which follow the optimal design criteria. Our study about the comparison of various interleaver design come up with following criteria that should exhibits in design:

- Interleaver should decorrelate the input elements as for as possible to acquire maximum value of 'spread'. In other words, how it will convert the bad codewords into good codewords.
- Interleaver should avoid identical permutation to minimize regularity in interleaving of input elements to improve the interleaver 'dispersion'.
- Last but not least, interleaver design should be memory efficient for application that requires minimal memory; this will also improve and ease hardware implementation.

### 2.3.2 Random Interleavers and Its Literature Review

Random interleavers are designed to randomly permute/ scramble the input bits/symbols. Interleavers are processes or functions that permute the input bits/symbols and can be written as:

$$C(i) \rightarrow \pi(C(i)) \quad (2.1)$$



where  $C(i)$  is the inputs data bits/ symbols and  $\pi(C(i))$  is the interleaved or permuted data bits/ symbols and  $\pi$  denotes the interleaver function.

Random interleavers are designed in such a way that it optimally breaks the continuous data bits/symbols with some degree of randomness in permutation. In order to evaluate the performance of random interleaver, it should have properties of 'spread' and 'dispersion'. These are discussed in the next subsection.

### 2.3.2.1 Random Interleaver Properties

#### a) Spread

Spread is an important property to fulfill the main design objective. For given interleaver/permutation function, one should find out the distance between the two values before and after the interleaving. In other words, spread compares the distances between the input values after interleaving and if interleaved values have greater distance then spread will be large and vice versa. Spread is the maximum value of  $S$  such that

$$|i - j| < S \text{ implies } |\pi(i) - \pi(j)| > S, \quad \text{for } 1 \leq S \leq N \quad (2.2)$$

where  $N$  is the total number of elements to be permuted. The first term in the above equation represents the distances between input elements before interleaving, and the second term the distances between input elements after interleaving. The two distance pairs, before and after the permutation of input data bits/symbols is compared with selected value of  $S$  to achieve high spread values. For example, let the distance between two values is (1, 1), before and after the permutation respectively. Now select spread factor  $S$ , say 2. By seeing the differences, it fails to satisfy the second term in Equation 2.2. That is because,  $1 < 2$  yet  $1 \geq 2$  is not satisfied. Therefore, the maximum possible spread is 1. In the same way, distance pairs for all elements are compared. To meet the system requirements, spread factor can be varied up to  $N$  (total number of data bits/symbols).

### b) Dispersion

Dispersion measures the randomness in interleaving. In other words, it measures the irregularity introduced by interleaver. The high dispersion denotes that variety of spread/permutation distances in input bits/symbols. To compute the dispersion, list of distances pairs of data elements must be calculated first. For given interleaving function  $\pi$ , the list of differences of  $\pi$  is defined as

$$D(\pi) = \{(j - i, \pi(j) - \pi(i)) \mid 0 \leq i < j < N\} \quad (2.3)$$

where  $D(\pi)$  denotes the dispersion pairs, and  $(j - i)$  and  $(\pi(j) - \pi(i))$  are the differences of input data bits/ symbols before and after the interleaving respectively. To understand the dispersion computation, let's consider the input data elements and its corresponding interleaved data as follows:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 4 & 1 & 5 & 6 \end{pmatrix} \quad (2.4)$$

First of all, list all difference pairs; compare the difference between input elements and differences after the permutation such as:

$$D(\pi) = \left\{ \begin{array}{cccccc} (1, -1) & (1, 5) & (1, -3) & (1, -3) & (1, 4) & (1, 1) \\ (2, 4) & (2, 2) & (2, -6) & (2, 1) & (2, 5) & \\ (3, 1) & (3, -1) & (3, -2) & (3, 2) & & \\ (4, -2) & (4, 3) & (4, -1) & & & \\ (5, 2) & (5, 4) & & & & \\ (6, 3) & & & & & \end{array} \right\} \quad (2.5)$$

In all pairs, first term denotes the difference before interleaving and second term denotes the difference after permutation. Looking at the first two pairs, the differences in input elements before is 1 and the differences after the permutation is -1, and 5 respectively. Following the dispersion property, repeated pairs are ignored. The pair (1, -3) is repeated



and has to be ignored. Now there are 20 elements pairs in total. In other words,  $|D(\pi)| = 20$ .

The normalized dispersion can be given by:

$$\frac{|D(\pi)|}{\binom{N}{2}} = \frac{2 \times |D(\pi)|}{N \times (N - 1)} \quad (2.6)$$

For above example the normalized dispersion will be:

$$\frac{2 \times 20}{7 \times 6} = \frac{20}{21} \approx 0.95 \quad (2.7)$$

The maximum value of dispersion is 1, so closer the value to 1, more disperse the permutation is.

### 2.3.2.2 Literature Review

Interleaver is mainly used in wireless communication system to handle the burst of errors introduced due to fading channels. The work on interleaver design is quite scattered in literature because interleaver is not specifically design for one application. The objective of interleaver in wireless communication system is to deal with burst of errors and to maximize the performance by converting maximum number of burst errors into simple errors which are corrected by using simple error correcting codes. Some applications have hardware limitations and that's why required optimized design that should minimize system complexity. The theory of interleaver was initially established in two classic papers [J. L. Ramsey et al. 1970] [G. D. Forney et al. 1971]. Elias in [P. Elias et al. 1960] originally pointed out that the interleaving can be useful to minimize errors, in transmission, on channels with memory. In the same era, work also had been undertaken for burst error correcting codes for bursty channels [I. S. Reed et al. 1960].

To fulfill the main design objective, block and convolutional interleaver are exploited with block and convolutional codes respectively. The most organized theory of interleaver parameter that characterized the behavior like complexity, delay, latency and



period for block and convolutional interleavers has been given in [K. Andrews et al. 1997], and later also established and cited in [R. Garelo et al. 2001]. In this paper, author analyzed the main parameter that characterizes an interleaver. As well, analyze the complexity for convolutional and block codes with said interleaver parameters.

In 1979, Philips Corporation of Netherlands and Sony Corporation of Japan defined a standard for the digital storage and reproduction of audio signal known as the *compact disk (CD) digital audio system*. There are several sources of channel errors introduced in CD, unwanted particles or air bubbles in plastic material, fingerprints and scratches during the handling. It is difficult to assume that how, on average, a CD will get damage. It is assume that the channel mainly has burst like error and these errors leads to several consecutive data samples in error [H. Hoeve et al. 1982]. The concept of interleaving is used here to rearrange the bits in time, so that the digits stemming from contiguous sample of the waveform are spread out in time. Following the same concept, interleaving also exploited in multimedia file transmissions [B. Sklar et al. 1988].

The design of random interleaver is an active research area and much efforts has been dedicated on random interleaver design since the introduction of parallel turbo codes based on binary systematic recursive convolutional constituents. The work in [S. Dolinar et al. 1995] described various interleaver design criteria's, and show that how the performance of turbo code is affected with the design of random interleaver. Moreover, random interleaver also acts as a key component in multimedia file transmission [A. B. James et al. 2004].

The detail literature review on random interleaver design based on its properties and design complexity tradeoffs are discussed as below:

- The earlier study on random interleaver was done by Ramsey on optimum interleavers for finite length sequence [J. L. Ramsey et al 1970]. Author proposed an interleaver that guaranteed input separation  $n_1$  and an output separation of  $n_2$  with minimum delay equal to  $n_2 (n_1 - 1)$ , where  $n_1$  and  $n_2$  are two positive integers satisfying  $n_2 < n_1 < 2n_2$ ,  $n_1$  and  $n_2 + 1$  are relative

prime. The separation guaranteed by Ramsey interleavers has been later named spreading after the invention of turbo codes.

- The families of random interleaver include S- random or semi random interleaver proposed by [D. Divsalar et al. 1995]. Author analyzed and compared the random and non- random interleavers and its effect on the design of turbo codes. Furthermore to analyze interleaver spread, various mathematical models have been derived to identify optimal interleaver for turbo codes. The spread of interleavers depends on the interleaver design criteria.
- Semi random interleavers are designed by keeping fix interleaver size that ensures the optimal performance with high interleaver spread. Consequently, some communication system requires flexible coding size, data rate and modulation schemes, that needs flexible interleaver size. Till that time, only fixed size interleaver has been used in various applications and that follows specific design method. As a result, interleavers are required with different size to fulfill the specific design objective. In order to deal with mentioned problem and to optimize the complexity of the interleaver design, pruning of interleaver was proposed by [M. Eroz e. al. 1999]. The proposed design is analyzed by taking block interleaver with pseudo-random readout to show that the performance of given interleaver is kept constant under severe pruning. Following the concept, pruning of interleaver has also been done for specific system design with given coding scheme [F. Danesgaran et al. 2004]. The concept of pruning was introduced for semi random interleaver by [M. Ferrari et al. 2002]. In this paper, author proposed an algorithm by modifying original semi random interleaver in order to prune down to smaller size by keeping good spreading property when pruned, furthermore complexity of interleaving using such technique can also be reduced. Flexible length semi random interleaver designed by Ferrari works well only to design small size pruning using larger interleavers. Consequently, large size interleaver can be generated



but leads to poor spreading property. To deal with large size interleavers keeping good spreading properties, Dinoi in [L. Dinoi et al. 2003] proposed a method of generating interleaver of any size by keeping good spreading property. Author compared the proposed interleaver with other interleavers in term of spreading property, distance, and claimed that variable sized interleaver can be generated with good spreading property. Consequently, storing all the interleaving patterns will also increase the complexity and degradation of performance for the system. Improving the interleaving spreading with optimal interleaving, semi random interleaving method has been proposed by [W. feng et al. 2002] and Danoi. Inspired from the algorithms proposed by Dinoi and Feng, Trifinal in [L. Trifinal et al. 2007] analyzed various interleavers and their convergence with different spread factor  $S$ . In this paper, author find out the probability of having different spread values and their convergence time with specific spread value.

- To optimize complexity of the system and keeping good random interleaving properties pruning based interleaver has also been optimized. Such work to optimize pruning based interleaver has been done by [P. Popovski et al. 2004] and [L. dinoi et al. 2005]. Accordingly, Interleaver designed in random way has greater performance with any interleaver size and keep good properties of spread and dispersion. Earlier, pruning of interleaver for smaller and also for larger size interleaver is described in the context of its spreading property. Randomness in spread also known as interleaver dispersion also been taken into account in the design of pruning of interleaver and analyzed by [L. Danoi et al. 2005]
- Semi random interleavers have been successfully employed in many systems, but surrounded by some disadvantages. The main problem that semi random interleavers possess is that they are not memory efficient. Consequently, these are expensive and infeasible for those applications that have minimum storage. It results in increase in complexity and degradation in interleaver



spread for large size interleaver. By means of pruning, interleaver for shorter/longer size can solved the above problem to some extent but still it acquire inherent memory problem of storing interleaving sequences. Hence, in order to construct simple and memory efficient interleaver, algebraic construction of random interleaver was proposed. The interleaving patterns are generated with minimum input parameters without storing the position of elements in memory.

- Alternatively, interleaver constructed algebraically is proposed [C. J. C. Bravo et al. 2004]. Algebraically constructed interleavers are memory efficient because its interleaving patterns are completely defined mathematically with minimum seeding parameter [J. Li et al. 2002] [K. Xie et al. 2006]. Moreover, it can perform as good as random interleaver. The deterministic interleaving patterns generated with algebraic interleavers are based on input seeding parameter so no need to store all interleaving patterns in memory and improves the memory requirement. Moreover, input seeding parameter that generates the interleaving sequences improves the interleaving complexity. The class of famous algebraic interleaver proposed by [C Heegard et al. 1999] [O Y takeshita et al. 2000] called *Welsh Costas interleaver* and *takeshita Costello interleaver* respectively. Both interleavers have good performance comparable to random interleaver and efficient performance, but *Welsh Costas* possess high complexity in design procedure and not practically design to follow all interleaver sizes. Furthermore, *Costello interleaver* has not complied algebraic construction and interleaving pattern is also not directly from input parameters [K. Xie et al. 2006]. Xie proposed cheap, simpler and easy to design *regular co-prime interleaver* using search tool named as *cyclic correlation sum* and compared this with various random interleavers and showed that the proposed algebraic interleaver work as good as random interleaver. Furthermore, it follows the algebraic design with permutation polynomials using integer rings discuss in [O. Y Takeshita et al. 2006].

- Algebraic interleaver performs as good as random like interleaver with simpler design, memory efficient for applications with minimum memory. But unfortunately, it cannot guarantee good random interleaving properties. The algebraic interleavers input parameters can be changed to generate varying interleaving patterns. The properties of random interleaver known as 'spread' and 'dispersion' can be improved with optimal design of algebraic interleaver. By keeping in mind the design implications, one need to design the interleaver to maintain good random interleaving properties [Kai Xie et al. 2006]. The random interleaving properties are also discuss in [O. Y. Takeshita et al. 2000].
- Algebraic interleaver subsequently outperform random and semi random interleaver in terms of complexity and ease of hardware implementation. The design of algebraic interleavers are also completely application specific as described earlier. The design is optimum in the sense that it concentrate to specific design requirement depending on application. Unfortunately, algebraic interleavers do not have good random interleaving properties. In [C. A. León et al. 2004], author designs an algebraic interleaver with monomials and analyzed the properties of random interleaver. The properties are analyzed, improved to some extent by varying input indices that affect the random properties [Y. B. Luis et al].

Review of all above interleaver showed that the design of interleaver depends upon application. Furthermore it should retained efficiency in term of design complexity, memory efficiency, and random interleaver properties for optimal interleaving in communication system. In other words, memory efficient, simpler design with good random interleaving properties should be required.

We conclude this section by highlighting the design of various interleavers that has been used and also still used by some systems. The first class and modified form of random interleavers are called the semi random or spread interleaver. The spread interleaver fulfills the main design objective with good random properties called 'spread' and 'dispersion' at the cost of saving all interleaving patterns. In order to design memory



efficient with minimal complexity, algebraic construction of random interleaver is proposed. The varying design criteria of algebraic interleavers proposed in literature, in some cases are unable to comply with efficient design criteria in term of complexity. Algebraic interleaver is step forward to optimal design criteria, but fails to achieve good random properties and design for specific application to attain optimal performance.

## 2.4 Security Implication

The typical advantages of pseudo random interleavers lies in the fact that the interleaving patterns are govern by pseudo random source used by interleaving methods to generate unpredictable interleaving patterns. The pseudo random source based on initial conditions/seeds used as a key to generate random sequence exploits known laws or methods to generate the sequences and these generated interleaving sequences are unpredictable. When these input seeds are used to initialize random sequence then given methods should utilize these random sequences in such a way that it produced interleaving patterns that are unpredictable and can be used as secure patterns if these patterns are kept secure and, additionally, these patterns eventually leads to have inherent optimal interleaving properties.

In order to generate secure interleaving patterns, following two points should be considered.

- Firstly, the choice of random source should generate unpredictable sequence with small change in initial conditions/seeds. Later, these random sequences are used to generate distinct interleaving patterns.
- Secondly, given random sequences should be exploited to generate interleaving sequence in such a way that the property of unpredictability in sequences remains after interleaving. In other words, the interleaving methods exploits random source in such a way that it acquires unpredictability after interleaving and not leads to same interleaving patterns with different random sequences.



By combining the ingredients of both selected random source and chosen interleaving methods, one can generate interleaving patterns having both optimal interleaving properties and possibly introduce security to make de-interleaving infeasible with different seeds. Moreover, who doesn't know the input seed or sequence cannot deinterleave the input data elements. The selection of random source is key ingredient to make good unpredictable sequence. Moreover, the variation of seeds to achieve different interleaving pattern, which solely depends on the chosen methods, makes the system more robust and introduce greater randomness in sequences and security.

Finally, it implies that pseudo random ways to generate random interleaver can produce low cost, easy to implement and secure interleaving patterns. In [J. Krhovjak et al. 2006], author has given comprehensive overview and analyzed various properties of pseudo random sequences. To consider security aspects, various cryptographic attacks on pseudo random sequence are also analyzed. The design of pseudo random interleaver should have inherent properties and can be taken into account as a good candidate to serve as security device.

## 2.5 Wireless Security Preliminaries and Related Literature Review

WLAN is not physically connected as wired LAN and is considered inherently insecure. Therefore, open invitation to eavesdropper to mount number of denial of service (DoS) attacks and leads to the disruption of available services for the users. The DoS attacks on MAC layer and upper layer are discussed later. The objective of this literature review is to go through various security mechanics and mechanism that are designed for wireless LAN and pin point various possible attacks on WLAN and suggested countermeasures.

Typical model of encryption and decryption will be discussed first. The key mechanics and mechanism exploited in WLAN are also presented. Based on these mechanics and mechanism, detail literature review on WLAN security to understand the security weaknesses will be discussed along with the key security threats currently faced by WLAN.

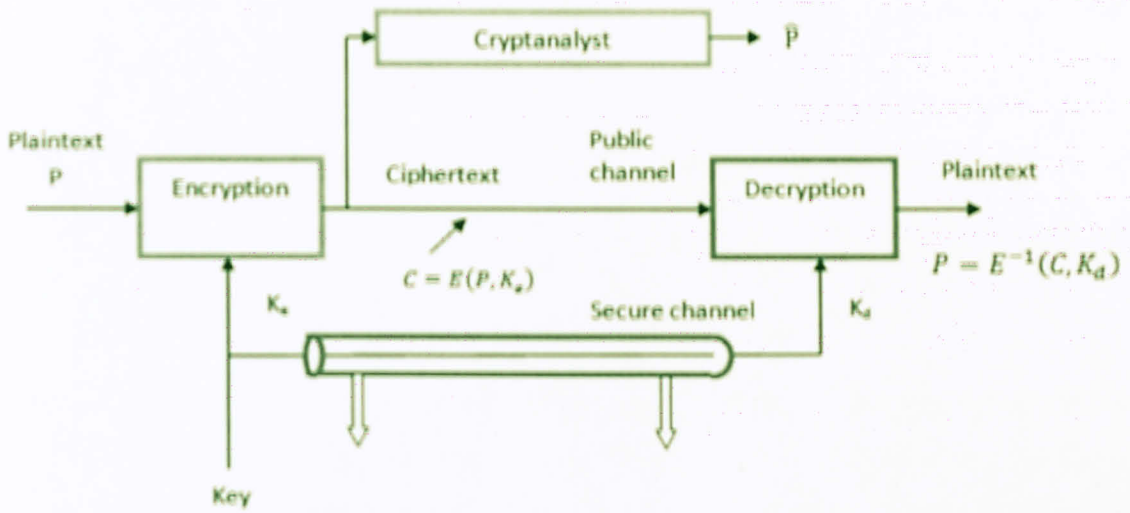


Figure 2.4: Typical model of encryption and decryption

### 2.5.1 A Typical Model of Security

The history of secure communication gives great invention, so that modern era sees through and tries to come to the point where security of the system cannot be compromised. In this section, detailed model of encryption and decryption will be discussed to facilitate the discussion in the thesis.

- **Cryptography:** the study of how to design a good encryption algorithms to disguise the input information and convert it from its normal, comprehensive form into an incomprehensive form and make it unreadable without secret key.
- **Encryption:** encryption is the transformation process of obscuring information at the transmitter to make it unreadable without secret key.
- **Decryption:** decryption is the inverse transformation process of converting back the obscured information into readable format with secret key.



- **Cipher:** cipher is an algorithm for performing encryption/decryption. It can also be referred as cryptosystem. Accordingly, the encryption algorithm is called *encipher*, while the decryption algorithm is called *decipher*.
- **Message – M:** the input to encipher is called message of plaintext  $P$ .
- **Ciphertext – C:** Ciphertext is the encrypted messages at the out of encipher and an input decipher.
- **Key – K:** A set of numbers/parameters that determine the specific encryption mechanism. Knowing the secret key enables message decoding. It is assumed that all aspects of an encrypted scheme are known to the unauthorized receiver, except the secret key –  $K$ .

In Figure 2.4 typical encryption model/scenario is illustrated. A message  $M$ , or plaintext  $P$  is encrypted by the use of invertible transformation using the key  $K_e$  and that will produce the ciphertext  $C = E(P, K_e)$ , where  $K_e$  is the encryption key. The ciphertext is then transmitted over insecure or public channel. When an authorized user obtains ciphertext, he decodes message using ciphertext  $C$  and the key  $K_d$  by applying inverse transformation,  $P = E^{-1}(C, K_d)$  where  $K_d$  is the decryption key.

As a whole, the security of cryptosystem is dependent on complete encryption process, but the design of the cryptosystem based on the algorithm and encryption transformation could be publically known. Hence, the security of the cryptosystem depends on the specific key. There are two ciphers following the relationship of  $K_e$  and  $K_d$ , when  $K_e = K_d$  the cipher is called a private key cipher or a symmetric cipher and when  $K_e \neq K_d$ , the cipher is called public key cipher or asymmetric key cipher. For private key cipher, the encryption and decryption key must be transmitted from sender to the receiver via a separate secret channel. For public key cipher, the encryption key  $K_e$  is published, and the private decryption key  $K_d$  is kept private, for which no additional secret channel is needed for key transfer. The public key ciphers are generally used for carrying the secret key  $K$  for the symmetric or private key ciphers.



### 2.5.2 Security Requirement

The requirement of security varies with application. The essential requirements are confidentiality, data integrity, authentication and availability. These four basic security mechanics are discussed in next subsection.

#### 2.5.2.1 Basic Security Mechanics

The complexity of securing wireless network can be well understood by discussing security mechanics available and used by wireless networks. The basic security mechanics discussed below describe the strength of wireless network. Moreover, these security mechanics can be achieved through implementing suitable technologies and designed protocols.

- a) **Confidentiality:** the main goal of confidentiality is to protect information after transmission from eavesdroppers, until it reaches the desired user. In other words, data confidentiality provides strong secure channel to protect information from unauthorized access. In order to do so, encryption is the key mechanism to provide data protection. Confidentiality is an effort to make the data meaningless for unauthorized party. Therefore, make it impossible for eavesdropper to capture the frames and acquire useful information. Data encryption is the key to provide confidentiality with well designed cryptographic algorithms.
- b) **Integrity:** data integrity responsible to check tampered data in transmission. Therefore, it is an effort to make it possible that the data transmitted to desired user is trustworthy and not altered on the way. This can be done with some integrity check mechanism to detect and correct the change made by eavesdropper. Digital signature a public key mechanism preferably used for data integrity.
- c) **Authentication:** Determines the identity of user, device or service available in the network with some pre- defined manner. The network must provide strong

authentication, so that communication parties authenticate each other's identity. Since, wireless transmission available to everyone in the range, much attention should be given to authentication in order to validate user, service and device. Authentication makes it possible that the user, service or device that has tries to access the network is authorized identity. Strong authentication should also require key generation, distribution and management used by cryptographic function. The authentication protocols can be designed in such a way that suitable and flexible authorization and access control strategies could be deployed to facilitate authorized users.

- d) Availability:** availability requires that the system should be robust and available for valid users at any time. In order to satisfy this, all defined security requirement should meet the goal. Availability is the capability to send and receive data at any time without interruption. Denials of Service (DoS) attacks are the serious threat to the availability of the network. Countermeasures should be taken in order to prevent or mitigate these DoS attacks to ensure the availability achieved.

### 2.5.2.2 Wired Vs Wireless

In the beginning, the security technologies were developed for wired network. However, with the passage of time wireless networks have more security challenges. The comparison of wired and wireless in context of security challenges due to their different characteristics is given below.

The first problem, in other words, inherent problem with wireless network is the availability of wireless medium. The wireless transmission is open to everyone specially intruders who tries to take advantages and misuse private information. In wired LAN, it is possible to hide the wires underground or inside the walls and restricts the access for outsiders. However, in wireless LAN it is very difficult to secure the transmission by changing the shape or limiting the radio transmission range. An outsider can try his luck



with openly available data because it is not necessary for him to connect with jack as in wired LAN. An attacker can connect by sitting far away with available tools.

The second problem with the wireless LAN is the authentication of the network. In wired LAN, user has some confidence on the validity of the network. For example, when user plugs his device he knows that the network is trusted as provided by trusted organization. On the other hand, in wireless network a user is completely blind of the connected network, because user can only see and trust the information Access Point (AP). The AP is invisible to the user and may be malicious.

The third problem with wireless LAN is related to the vulnerability of wireless link with the environment. The environment causes high loss rate and bit error rate (BER). Hence, protocols should be designed to enhance the performance of wireless network and make it possible with as minimum loss and damage as possible.

The advantage of wireless network is the mobility of the user device, flexibility and adaptive choice of the network depends on the link quality. Finally, in order to improve the transmission in term of power, complexity and security; the protocols should be efficient and scalable to support user mobility.

### **2.5.3 Security Threats**

Wireless LAN is intrinsically insecure as compare to the wired LAN. It is difficult to prevent access to the wireless network as it works through the air. Anyone in the middle can capture the transmitted signal in the range with available tools. To improve the security, it is important to analyze the security protocols to understand the likely capabilities of the attacker. For client and access point negotiation and data transmission, three types of frames: management, control and data frames are used. Any manipulation of these frames gives rise to number of attacks. In the following, we outline the attacks which jeopardize the WLAN transmission.



**Threat 1: Passive Eavesdropping and Traffic Analysis**

Wireless LAN is susceptible to attack and attacker easily sniffs and stores the wireless transmission. In passive eavesdropping, an attacker silently monitors the wireless traffic without changing the contents of transmission. There are two methods deployed to execute undetectable passive attacks: eavesdropping and traffic analysis. Eavesdropping is the capability to monitor the transmission for message contents. Attacker tries to find out the source and destination address, burden on network and time of transmission. Traffic analysis is the capability to gain intelligence by monitoring transmission for pattern of communication, or perform packet analysis. The undetectable sniffing performs two key functions: packet capture and packet analysis and display. Analyzing a packet determines the capability of the network i.e. security protocols used by the network, client and access point (AP) capabilities. With packet capture, an attacker tries to exploits the confidentiality. There is wide variety of sniffing tools available, both on the commercial market and through open source. In 2001 Shipley [P. Shipley et al. 2001], invented the first 'War Driving' used to investigate the network. It can discover the AP, the corresponding Service Set Identifier (SSID) or even the physical location of AP with moderate equipment. An attacker can get sensitive information and exploits the bandwidth for free access if the AP is not well configured.

**Threat 2: Active Eavesdropping and Message Injection**

Active eavesdropping is more dangerous than passive eavesdropping. In this, an adversary is capable of inserting a message into the wireless network using moderate equipment, device with common network interface card (NIC). First of all, an adversary investigates the wireless network capabilities using passive eavesdropping, then by active eavesdropping. Using the unprotected information i.e., MAC headers, management and control frames, an adversary can control any field. Hence, it reasonable to assume that adversary can generate any chosen packet, modify the contents of the packet and completely control the transmission of the packet. If packet needs to be authenticated, an

adversary breaks the authentication mechanism and also exploits the integrity mechanism by playing with the packet fields. In [J. Bellardo et al. 2003], detailed analysis of possible attacks on WLAN to exploits the security protocols is given. In order to identify the expediency and effectiveness of these attacks, software infrastructure using commodity hardware is used to initialize these attacks by generating arbitrary frames.

### **Threat 3: Message Deletion and Interception**

In this attack, an adversary is capable of message deletion, means that adversary can intercept and remove message from the network before it reaches to the destination. The contents of the message modification can cause the packet deletion at the receiver. This could be done by interfering with the packet reception mechanism at the receiver antenna, for example, causing Cyclic Redundancy Check (CRC) error so that receiver drops the packet. This can also be caused due to noise in the transmission, but may be initialized by the attacker.

Message interception means that an adversary controls the connection completely. In other words, an adversary can capture the packet, and then decide whether to delete the packet, modify or send to the receiver. This is more dangerous than eavesdropping because the receiver does not get the packet before the adversary forward it. But in WLAN, message intercept is seems difficult because receiver will receive the packet before the adversary does so. But an adversary can achieve packet interception with some potential ways. First, directional antennas can cause a packet to delete at receiver side by causing collision, than at the same time use another antenna to receive the packet. The message interception is difficult to achieve by the attacker, we consider this if damage caused is more brutal. For message interception, there is no need by the attacker to initialize man- in- the- middle (MitM) attack.



**Threat 4: Masquerading and Malicious AP**

In this attack, an attacker disconnects the user by sending disassociation and de-authentication forged frames, and forced the user to associate with forged AP by showing high signal strength. By doing so, an attacker have all the legitimate user credentials and private data i.e., passwords and also intelligently, adversary tries to find the encryption key by exploiting the confidentiality protocol. This is all because, the plaintext MAC addresses are included in the frames transmitted through wireless link. The adversary can learn the valid MAC addresses, and modify these to any extent because the firmware provides the interface. An attacker knows the source and destination MAC address to masquerade as legitimate user or legitimate access point. The adversary can install his own AP using forged MAC address and spoofed SSID. With this, adversary can find a backdoor to enter the network.

**Threat 5: Session Hijacking**

This attack is capable to redirect network traffic away from a legitimate end user. An attacker has the ability to sniff and insert his own information. We consider that an adversary may hijack a legitimate session after wireless device have finishing authenticating themselves. First, an adversary knows the capabilities of both devices by sniffing the beacon frame or probe request frame, then masquerade as legitimate user by spoofing the MAC address given in unprotected management and control frames. An attacker sends forged disassociation and de-authentication management frames to forcibly disconnect the user from AP, and associate with AP with spoofed MAC address. This attack possibly avoids the authentication mechanism. Moreover, it can also try to exploits the confidentiality and integrity protocols to get transmission data or in order to initialize DoS attacks.



**Threat 6: Man – In – The – Middle – Attacks**

In this attack, an adversary must participate in communication continuously. If there is transmission going on between clients and access point, the adversary must break this and masquerade as legitimate user and access point. In order to do, an adversary spoof the unprotected management frame, modify its contents and send it to the recipient. For AP he acts as legitimate user and connect legitimate user with rouge AP. This can be easily done by using NIC cards one as program legitimate user spoofed MAC to connect with AP, and other as rouge AP to connect legitimate user. In that case, both legitimate user and AP fail to detect the intruder and continuously transmits the information.

**Threat 8: Denial of Service Attacks (DoS)**

WLAN is quite vulnerable to DoS attacks. This attack prevents legitimate user to access network resources. DoS attacks are most devastating and difficult to prevent. The worst scenario for WLAN due to all attacks given above is DoS attacks. DoS attacks can disrupt services for a single user or for the whole network. End results can include an attacker a means to setup a rouge AP and associate users to bogus network (MitM attack), to completely shut down the network not allowing any transaction to take place. The aim for DoS could be

- Deploying radio jamming equipment.
- Saturate the network bandwidth filling the AP authentication and association queue by continuously sending the management frames.
- To disrupt the legitimate user traffic by sending the forged disassociation/de-authentication management frames.
- Forged RTS/CTS control frames to conduct transmission duration attacks configuring the transmission duration field to maximum of 30 packet/second.

The detailed analysis of DoS attacks is given in [J. Bellardo et al. 2004]. This paper shows the practical strength of DoS attacks on forged management frames (includes

disassociation /de-authentication attacks) and on control frames (include power save attacks on polling message and media access attack on RTS/CTS/ACK control frames).

#### 2.5.4 Related Literature Review on Wireless Security

In the beginning, the main objective of the researchers was to secure the information data transmitted by the clients as good as wired LAN. In order to provide data confidentiality and integrity, the IEEE 802.11 standard [IEEE 802.11, 1999] comes with the wired equivalence privacy (WEP) to provide same data protection as wired LAN. This mechanism adopts common stream cipher known as RC4 (Rivest Cipher 4) [B. Schneier et al. 1996], to encrypt the data with shared key. This key is concatenated with 24 bit initialization vector (IV) to construct per packet RC4 key. For data integrity, WEP calculates integrity checksum value (ICV) over MAC service data unit (MSDU), which is cyclic redundancy checksum (CRC). The key sequence and ICV generated data are XORed to obtain cipher text. Furthermore, two authentication mechanisms are also defined: the open system authentication which is actually null authentication, and shared key authentication, which is based on challenge response handshake on shared key.

Initially, IEEE 802.11 claims that WEP is reasonably strong to provide data confidentiality, integrity and authentication. WEP is self synchronizing, meaning that it automatically encrypts all frames when the WEP option is turned on. The WEP is also become popular due to ease of implementation on hardware and software on wireless devices, which have limited computational power as compared to wired LAN. However, study shows that data confidentiality, integrity and authentication are not achieved using these mechanisms and WEP has inherited flaws. First, the 40 bit key size is too short for brute force attack [N. Borisov et al. 2001] [J. S. Park et al. 2004]. Furthermore, the initialization vector (IV) is public and has small size; it is easy for the attacker to partially or completely recover the plaintext by applying known plaintext attack and static key [N. Borisov et al. 2001][J. R. Walker et al. 2000]. The data integrity is also compromised because the ICV is linear and un-keyed function of the message [N. Borisov et al. 2001]. The integrity also cannot be guaranteed; the adversary can modify the message without detection, and forge the packet with a valid ICV, even without the knowledge of the key.



Furthermore, weak integrity enables attacker to easily recover the plaintext with chosen plaintext attacks [W. A Arbaugh et al. 2001(I)], and can also spoof the shared key authentication. In WEP, there is no mechanism to protect the shared key authentication. The adversary can trivially spoof the shared authentication [W. A. Arbaugh et al. 2001(II)][N. Borisov et al. 2001], through scrutinizing the authentication process of legitimate user. Additionally, WEP does not implement any mechanism to protect reply attacks. The WEP 128 bit is completely insecure and can be broken in 3 minute [H. Cheung et al. 2005]. In [N. Asokan et al. 2002], the authentication, confidentiality and integrity are analyzed and proposed two enhancements to improve authentication, confidentiality and integrity. The scheme cover the weaknesses of key stream by using private initialization vector (IV) and days/session keys to supply a higher key seed space resulting in lesser key stream reuse with some degree of computing cost. The researcher gives the solution to improve the WEP, but due to inherent flaws WEP needs to replace to improve the security.

Initially, security is concentrated only for data transmission, popped up security holes in 802.11 and WEP led to the development of new security standard. The evolution in security demands broader view to improve security towards authentication and integrity. In October 2003, the Wi-Fi alliance launched an interim solution named Wi-Fi Protected Access (WPA) to improve the vulnerabilities. The WPA adapted as much of the 802.11i [IEEE 802.11i/ D10i. 2004], so that WPA to be the strong economical solution that worked with both legacy hardware and forward compatible with the 802.11i.

WPA comes with improved data encryption, authentication, integrity and key management. To improve data confidentiality, WPA adopts Temporal Key Integrity (TKIP) algorithm that still uses RC4 algorithm for encryption, but improved key mixing and extended initialization vector (IV) space to generate fresh per packet keys. In addition, WPA provides two improved authentication mechanisms. In one mechanism, the possession of a Pre-Shared Key (PSK) authenticates the peers; furthermore, a 128-bit encryption key and another distinct 64-bit MIC key can be derived from the PSK. Alternatively, IEEE 802.1X [IEEE 802.1X- 2001] and the Extensible Authentication



Protocol (EAP) [L. Blunk et al. 2003] can be adopted to provide a stronger authentication for each association, and generate a fresh common secret as part of the authentication process; all required keys can be derived from this shared secret afterwards, these are also included in 802.11i just for backward compatibility, RSNA algorithms are proposed to provide scalable, flexible and strong securities in wireless networks.

The security standard IEEE 802.11i defines three data confidentiality protocols: wired equivalent protocol (WEP), temporal key integrity protocol and counter mode/CBC-MAC protocol (CCMP), the weaknesses of WEP and TKIP are studied in [W. A Arbaugh et al. 2001(I)] [W. A Arbaugh et al. 2001(II)] [M. Cam-Winget et al. 2003] [S. Fluhrer et al. 2001] [V. Moen et al. 2004] [J. S. Park et al. 2004] [A. Stubblefield et al. 2002] [J. R. Walker et al. 2000]. To make compatible with legacy hardware, WEP and TKIP used RC4 stream cipher. Unlike WEP and TKIP, CCMP uses CCM (counter with CBC-MAC) operation [D. Whiting et al. 2003] on AES encryption algorithm [NIST, FIPS Pub. 2001] with 128-bit key and 128-bit block cipher. The detailed analysis of 802.11i confidentiality and integrity protocol against key related attack, CTR overlap, and pre-computational is given in [Cisco Systems. 2001].

IEEE 802.11 defines authentication mechanism (open system authentication and shared key authentication) which is completely insecure [N. Borisov et al. 2001] [W. A Arbaugh et al. 2001(I)]. In order to provide strong authentication mechanism, IEEE 802.11i defines new Robust Security Network Association (RSNA) to provide strong mutual authentication and generating strong keys for data confidentiality protocol. RSNA defines a protocol using IEEE 802.1X EAPOL-Key Frame called the 4-Way Handshake which plays a very important role in authentication and key management. In order to analyze the security of protocol with 4-Way Handshake, a lot of work has been done [C. He et al. 2004]. In [F. Zhang et al. 2005], the security of 4-Way Handshake is analyzed using Canetti-Krawczyk (CK) model, a general frame work for constructing and analyzing authentication protocol in realistic models of communication network. This paper proves that 4-Way handshake protocol can satisfy the definition of Session Key (SK) [R. canetti

et al. 2002] in Unauthenticated-link adversarial Model (UM) and also the Universal Composable (UC) security.

802.11i RSNA establishment procedure consists of 802.1X authentication and key management protocols. Three entities are involved in transmission, called the Supplicant (wireless station), the Authenticator (the Access Point), and the Authentication Server (de facto a RADIUS server [C. Rigney et al. 2000]). In general, a successful authentication means that the supplicant and the authenticator verify each other's identity and generate some shared secret for subsequent key derivations. For secure data transmission session, key management protocol computes and distributes usable keys based on shared secret. The authentication server can be implemented either in a single device with the authenticator, or through a separate server

At present, the concern for researcher is the availability of WLAN. As the WLAN is not physically connected as wired LAN, wireless signals can be intercepted with moderate equipment. Now researcher tries to push the technology where the attacks on availability of WLAN are minimized. Previously, much effort has been devoted to improve the security protocol of WLAN. In [C. He et al. 2005] the IEEE 802.11i is analyzed for data confidentiality, integrity, mutual authentication and availability. This paper shows that, security standard 802.11i appears to provide effective data confidentiality and integrity when CCMP is used. Furthermore, 802.11i adopts a RSNA establishment procedure for mutual authentication and key management, which appears to be satisfactory secure. However, several vulnerabilities might arise in real implementation if mutual authentication mechanism is not suitable. There might be a MitM attack that reveals the secret key. This paper also analyzed the security rollback attack, reflection attack and RSN IE poisoning attacks which mount number of DoS attacks and disrupts the availability of the WLAN.

With the evolution of WLAN, demanding features and robust network security beyond data frames is necessary. The future of WLAN comes with the new standard which burden up management and control frames by extending the functionality with sensitive



information including radio resource data, location based identifier and fast roaming information. The secure transmission of these frames is necessary for reliable transmission. The latest security standard 802.11i improves the security with WPA2-complaint hardware. But still gap for attacker to disrupt the availability of the WLAN, leaving many DoS attacks. Moreover, these DoS attacks are severe due to unprotected information at MAC and PHY layer i.e., management, control frames and MAC headers. These frames are used to establish and maintain connection between clients. The frame header contains source and destination addresses, which is used to track the clients and route the traffic. The network card contains MAC address as identifier for the hardware. This address can be used to recognize the sender or receiver. An attacker utilizes the information to initialize number of DoS attacks even with the strong data authentication and confidentiality protocol is used. Considering the management frame attacks, the most efficient attack is to forge and repeatedly sends the de-authentication and disassociation frame. Furthermore, security rollback attacks on beacon management frames. At control frames, attacker targets the virtual carrier sense mechanism like Request To Send (RTS) frame [J. Bellardo et al. 2003][D. Chen et al. 2003]. Recent research analyze the de-authentication/disassociation attacks and other attacks that include rouge access point, beacon frame attacks to initialize various DoS and countermeasures for these attacks are proposed in [M. Malekzadeh et al. 2007] [C. Liu et al. 2008] [C. Liu et al. 2007] [A. Martinaz et al. 2008] [C. L. Shuba et al. 1997]

Previously, encryption is running on higher layer to encrypt the specific data. Services running on the lower PHY layer are left unprotected. At PHY layer, management and control frames used for addressing, synchronization and control information are left unprotected. Eavesdropper thus able to used unprotected MAC header, management and control frames for synchronization, resolves the addressing and control information. As a result, by using this information, eavesdropper may have the capability to read control information, cryptanalyzed the binary ciphertext later on to recover the key and still initialize number of DoS attacks to disrupts the communication.

### 2.5.5 Interleaver as a PHY Layer Security Device

The basic premise of interleaver that has been observed is to decorrelate the adjacent bits/symbols in such a way that the burst of errors should appear as random as possible. Furthermore, techniques employed to interleave the input data (feed as block, bits or packets) should known at the receiver side to efficiently restore the original data/sequence. Interleaving methods may consist of one function to interleave the transmission, or seed based design to permute block of data. In seed based design, changing the input seeds perhaps generate different interleaving patterns. So that, seed based design can be exploited and useful if the interleaver patterns generated based on seeds are equally likely. The generation of highly random interleaving patterns guaranteed the unpredictability of sequence and careful design of seed based interleavers to generate random sequence cannot be underestimated.

Primarily, generation of seed based interleaving patterns thereby introduced as PHY Layer security device. The property of such designs to generate varying sequences securely interleaves the coded data, while interleaving patterns are kept secure. Moreover, at receiver side all patterns can be recovered using same input seeds. Hence, input seeds to initialize interleaving methods are used as a key. In order to correctly recover the interleaving patterns, one need to know the correct key, otherwise it is infeasible to recover the correct sequence. Above all, to strengthen the security and also interleaver design, generated sequences should not reveal any information that expose the key or input sequence. To make these possible, interleaving methods should be designed in such a way that it generates unpredictable sequence with each input seed. In that way, precise choice of interleaver to encrypt the transmission data will significantly strengthen the security of data. In wireless communication system, interleaver as a PHY layer security device comes at no extra cost in terms of system resources, while it will helps to further improves the security of PHY layer data.

There are many layers that are used to secure the transmitted data. Previously, medium access control (MAC) layer and upper layer are considered for WLAN security. In typical wireless communication system, MAC layer considered as security layer to encrypt



information. For reliable data transmission at PHY layer, channel coding with interleaving helps to minimize errors intruded due to wireless channels. For secure data transmission at MAC layer, all the mechanics and mechanism of security is established. The element of security with seed based design at PHY layer is an effort to fill security holes at MAC layer. The design of interleaver with desired property that enhances the reliability and security transmitted data to a great extent, while further increases the cross layer security.

At higher layers, interleaving is also exploited independently for specific application as dual purpose: for reliability and security of data. In [J. I. Gao. et al. 2002] author proposed a technique to encrypt the audio data called hierarchical data security protocol (HDSP) for voice over IP (VOIP) at transport layer. Author employed two stage interleaving called: inter frame interleaving and intra frame interleaving. In order to maintain the voice quality degraded by packet loss due to burst noise, inter frame data interleaving is employed. Moreover, to improve the security of audio frames, intra frame interleaving is introduced.

### **2.5.6 PHY layer Security**

Previously, encryption is applied at bit stream level to secure only data frames at MAC layer. Earlier, emphasis is to strengthen the confidentiality of WLAN using given mechanisms to secure transmitted data. Therefore leaving management, control frames so that MAC headers unprotected at PHY layer. To ensure the data reliability, modulation, interleaving, channel coding and other known patterns are kept unprotected at PHY layer and used by receiver to recover transmitted information correctly. The attacker use these unprotected information contained in unprotected frames to extract encrypted bit stream to guess the encryption key or to disrupt the transmission. The building blocks for data reliability and transmission of PHY layer data patterns include channel coding, interleaving and modulation can be kept secret.

The introduction of PHY layer possibly helps to prevent attacks and strengthen overall WLAN security. In order to improve the security, some work has been reported in the literature for the purpose to improve and assist upper layer security.

- The unprotected MAC frames and so MAC headers are considered to be the main cause of attacks at PHY layer by revealing information. Considering the management frame attacks, the most efficient attack is to forge and repeatedly sends the de-authentication and disassociation frame. Furthermore, security rollback attacks on beacon management frames. At control frames, attacker targets the virtual carrier sense mechanism like Request to Send (RTS) frame. The analysis of mounted attacks on MAC frames that disrupt the availability of WLAN has been discussed in detail in [J. Bellardo et al. 2003][D. Chen et al. 2003].
- A security model to prevent attacks due to unprotected management frame is proposed and discuss in [M. Malekzadah et. al. 2007]. Author analyzes all possible attacks due to management frame and proposed new modified frame format. Mathematical probabilities are carried out for authorized and unauthorized source for frames and required time for collision and forgery attacks.
- Spread spectrum based communication system considered to have built in security as compared to other systems i.e., OFDM. Inspired by the fact that PHY layer enhancement has been proposed in [Hwang et al. 2004]. Author proposed chaotic direct sequence spread spectrum (DS/SS) over AWGN channel. The probability of error with intended and unintended receiver and performance enhancement for intended receiver based on the choice of chaotic map has been presented.
- Following the notion of previous DS/SS based communication system, PHY layer enhancement has also been proposed in [Ling et al. 2004]. Author proposed *chip level* secure interleaving for CDMA based system to improve performance in burst like environment and at the same time enhance the security measures.
- The enhancement for PHY layer of OFDM based communication system has been proposed in [Dzung et al. 2005]. Author proposed constellation scrambling to



secure services running on PHY layer of the system. The security of the system is based on the external key used to encrypt and decrypt the given data. Author claim that in doing so, attacker will not be able to acquire the encrypted signal without the knowledge of the key.

- The security for wireless networks also been proposed in [Pal et al. 2006]. In this patent, author proposed encryption and decryption of channel coding using convolutional encoder and viterbi decoder to provide security against known plaintext attacks. The ciphertext is obtained after channel coding using well known RC4 encryption algorithm. The choice of the seed as an input to encryption algorithm and generated out sequence be the merit of security for the system.

Therefore in the light of available literature, it is possible to introduce security at PHY layer. The introduction of PHY layer security helps to assist MAC layer and upper layers. Moreover, the unprotected information at MAC layer can be protected at PHY layer. With the PHY layer security not only protects upper layer data, but also protects services running on that layer. At receiver, without the knowledge of the key it is impossible to acquire any clue of received signal.

## 2.6 Summary

The background and literature review is divided in two parts. First part detailed the background and literature review of interleaver and second part devoted for the literature review of wireless security.

The introduction of wireless channel that disrupts the transmission of the system and induce errors that degrade the performance of the system is presented. Followed by the introduction and types of interleaver has been discussed. On the basis flexible design, random interleavers have been chosen and it is one of the active research area. Random interleavers do not follow specific design criteria for applications, but varies based on design complexity and performance. Random interleavers have properties of optimal

interleaving and are analyzed based on these properties. The work done on random interleavers has been detailed at the end.

Secondly, this chapter presents in detail the literature review on the issues to secure PHY layer of WLAN. First, the issues related to MAC layer security and countermeasure based on different types of attacks specially DoS and prevention of these attacks has been analyzed. Issues on PHY layer security and literature review on it at the last.



## Chapter

# 3

## Novel Seed Based Random Interleaver with Improved Performance: Design and Analysis

In chapter 2, literature review on random interleaver as well as its PHY layer security is presented. The importance of interleaver in improving the performance of communication system in fading channels that introduce burst errors is highlighted. The types of various interleavers in practice and their classification based on its design and performance have also been discussed. Interleaver is also considered as a key candidate as a PHY layer security device. Therefore, the security aspects of interleaver at PHY layer are thoroughly analyzed along with the discussion on optimal interleaver design to deal with burst errors due to fading channels. The wireless local area network (WLAN) preliminary concepts have been presented first to get familiar with the basic terminologies used. This is followed by various security threats in WLAN and related literature review that presents the strength of security attacks and appropriate countermeasure taken at MAC and higher layers. The security implications of interleaver as a PHY Layer security have been discussed.

This chapter discusses the research methodology of proposed seed based random interleaver for improved performance. The objectives of this research are discussed in section 3.1. Random interleavers are analyzed based on their properties of spread and

dispersion and also the performance in burst error environment. The performance measures to analyze the proposed SBR Interleaver are discussed in section 3.2. Seed based interleaving methods are initialized using input seeding parameters. With the knowledge of input seeding parameters complete sequences are recovered at de-interleaving. Moreover, SBR interleaver makes use of random sequences to generate unique interleaving patterns. The random sequences should be deterministic in nature so that interleaving patterns based on underlying interleaving methods are recovered successfully at the receiver end. The unique random sequences for proposed SBR Interleaver are generated using RAND function in MATLAB and also a chaotic sequence generated from Logistic function. Our proposed design has the property to generate unique patterns with given random sequence and has inherent interleaving properties. In other words, proposed SBR interleaver can generate interleaving sequences and has optimal interleaving properties with any random sequence. The entire design is explained in section 3.3. The performance of the interleaving properties spread and dispersion of the proposed design is evaluated using simulation. The parameters of the simulation and the analysis of the results are discussed in section 3.4. Similarly, the comparison of proposed SBR Interleaver with random interleaver in burst error environment is analyzed in section 3.5.1 with the help of bit-error rate as a function of length of burst errors. The introduction of SBR Interleaver in typical communication system and its suitability at bit level before modulation and at symbol level when it is introduced after the modulation is analyzed in section 3.5.2. Analysis of proposed SBR interleaver at pre and post modulation interleaver for OFDM system in burst error environment is given in section 3.5.3.

### 3.1 Objectives

In the light of the a typical communication system block diagram shown in Fig. 2.4, the objective of this work is to design and analyze the proposed seed based random interleaver that should result in the desired performance to be described in detail in section 3.2. The design and analysis of proposed seed based random interleaver is



described later in this chapter. The technical objectives of this chapter are to achieve the following:

- To design a novel seed based random (SBR) Interleaver to obtain near optimal performance in burst like environment.
- To show that proposed SBR Interleaver has good random interleaving properties of 'spread' and 'dispersion'.
- To analyze that the proposed seed based random interleaver has the generic design, in that the random interleaving properties of proposed interleaver is not dependent on the random sequences. To show that, random sequence is generated using two techniques, namely the MATLAB RAND function that is dependent on pseudo-random numbers and also chaos using well known chaotic logistic map (CLM).
- To show how efficiently the proposed SBR Interleaver spreads out the maximum number of burst errors into simple errors that will be entertained by simple single error correcting codes. The comparison of proposed SBR Interleaver is carried out with other random interleaver to show that proposed SBR Interleaver has the capability to convert good number of burst errors into simple errors as compared to other interleavers.
- To find out the suitability of proposed SBR Interleaver at bit level used in its usual position before the modulation and also at symbol level when it is introduced after the modulation. The comparison of pre- and post modulation is carried out to find out the complexity of interleaving at both locations.
- To show the performance of SBR Interleaver with pre- and post modulation design for OFDM system in burst error environment. For that purpose, complete

end to end WiMAX model compliant with IEEE 802.16d is developed and simulated in MATLAB.SIMULINK to evaluate the performance.

### **3.2 Performance Parameters of SBR Interleaver**

The performance of proposed SBR Interleaver measured in terms of bit error rate as a function of length of burst error when used in conjunction with single error correcting codes critically depends on its following two inherent parameters:

#### **3.2.1 Spread**

Interleaver spread is one of the properties and performance parameter of random interleaver. The spreading measures the distance between the elements those were close to each before permutation. For optimal performance in wireless communication, interleaver should have good property of spread. The interleaver spread has been discussed in chapter 2. Our proposed SBR Interleaver is designed to have very good spread.

#### **3.2.2 Dispersion**

Another related property and performance parameter of random interleaver is to find out the randomness in spread is called dispersion. Interleaver dispersion improves the regularity in interleaving to avoid bad codewords and to generate good interleaving sequences. Having both good spread and dispersion brings perfectness in interleaving.

#### **3.2.3 BER as a Function of Length of Burst Errors**

Finally, interleaver with optimal properties of spread and dispersion converts burst of errors into simple single errors and these are later corrected using single error correcting codes. Interleaver should have the capability to convert long burst of errors into simple random errors. Our proposed interleaver is compared with random interleaver to analyze the performance in burst error environment. The bit error rate (BER) is plotted against



numbers of burst errors to show the performance of interleaver in converting burst errors into simple errors which are corrected by single error correcting codes used in the system.

### 3.3 Design of Proposed Interleaver

Interleaver is a process to change the positions, or scramble input positions of data elements in any given input sequence. Interleaver is a kind of scrambler and is considered as a special case of scrambling. To interleave the input data elements, unique scrambling is carried out. Our proposed SBR Interleaver too basically generates a scrambled sequence with the help of suitably designed scrambling matrices. A scrambling matrix is an  $N \times N$  matrix with each row having all zero elements except one element whose value is '1'. The underlying logic is to generate scrambling matrix with unique random locations of '1' in each row. To interleave any given input sequence it is multiplied and position of '1s' will make a decision for new interleaved positions for the input elements. The utmost goal of the said design is to have optimal interleaving properties.

Generally interleaving sequences are transmitted and are made available for receiver to efficiently recover the transmitted data. Alternatively, interleaving sequences are kept secure in order to introduce interleaver as a PHY Layer security device. Therefore, proposed SBR Interleaver can be employed as PHY Layer security device. The suitability and security implications of interleaver as PHY Layer security device has been discussed in chapter 2. Secure interleaving can be employed at bit level or at symbol level. The bit level interleaving is performed on coded bits, so at bit level the size of interleaver is arbitrary. Similarly, the size of interleaver is also arbitrary when used post modulation. However, in case of OFDM systems, the size of the interleaver follows the size of FFT/IFFT. The possible advantage of symbol level interleaving in terms of reduced complexity and enhanced security will be discussed later. When the proposed SBR Interleaving is introduced at symbol level after the modulation, all services running on PHY layer will be protected against eavesdropping. The analysis of proposed scrambler as a secure interleaving device will be discussed later.

### 3.3.1 Scrambling Based Interleaver

The details given above pave the path to understand scrambling based interleaver. Interleaving is considered as a special case of scrambling. Interleavers are used in digital communication to avoid burst errors that override data elements due to long duration fades in fading channel. The scrambling/interleaving can be random, semi random or algebraically design. The question arise how interleaver improves the design and enhances the performance? To design interleaver optimally, it should spread out data elements in an optimal way. The interleavers that have been discussed and presented in previous chapter are mostly application specific and are designed keeping one or two design objectives.

The block diagram of proposed seed based scrambler is shown in Figure 3.1. The input seeds or states, shown in the figure, are used to initialize a random number generator (RNG). The unique random sequences are generated with random number generator and initialized with input seeds. There are various random number generators that can be used here. In this work, two random sequences are considered. The random sequences are generated using pseudo random sequence with RAND function in MATLAB® and chaotic sequences using chaotic logistic map (CLM) as shown in the Figure 3.1.

The block diagram of proposed scrambler consists of two inputs. Firstly, the input data elements  $X_i$  are fed in parallel as a column vector as below:

$$X_i = \{x_1, x_2, x_3, x_4, \dots, x_N\}' \quad (3.1)$$

The above equation shows the  $N$  input data elements column vector.

The interleaving pattern that is generated using SBR Interleaver actually corresponds to interleaved positions of input data elements. Furthermore, the underlying logic behind is to design scrambling matrix as shown below:

$$S = \{P_1, P_2, P_3, \dots, P_N\}' \quad (3.2)$$

where  $S$  is the scrambling matrix and  $P_i$  is the  $i^{\text{th}}$  position row vector among  $N$  position row vectors for  $N$  input data elements



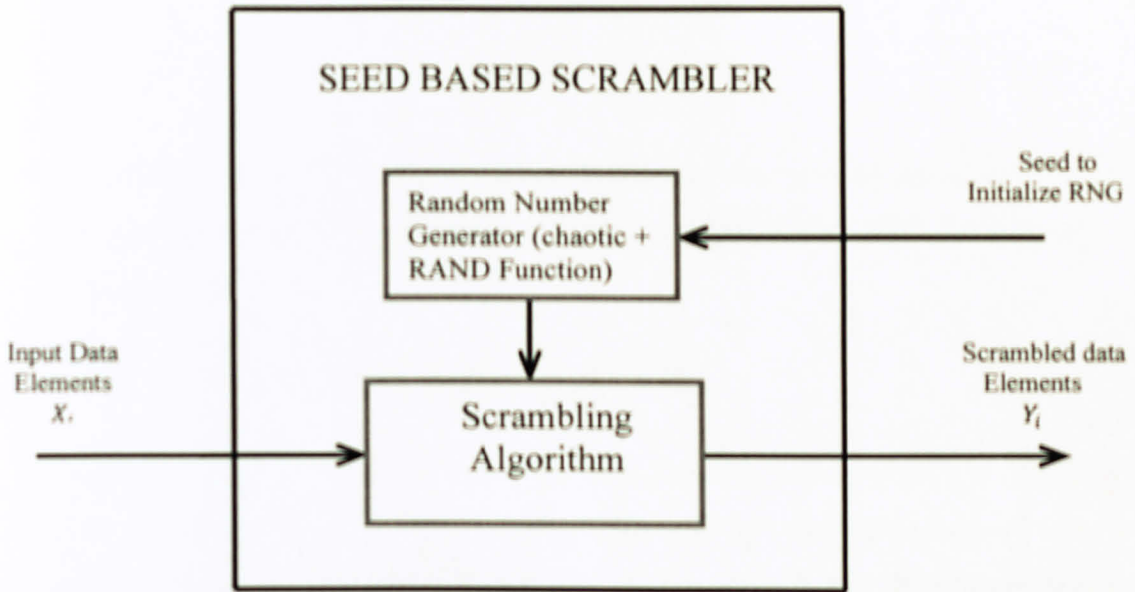


Figure 3.1: Block diagram of seed based scrambler design

The scrambling matrix can also be written alternatively as;

$$S = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad (3.3)$$

and each row in the scrambling matrix  $S$  correspond to position row vector  $p$  and the location of '1' in  $i^{th}$  position vector correspond to the location  $i^{th}$  input data element after scrambling. The diagonal scrambling matrix corresponds to same position before and after the scrambling.

In order to achieve  $Y_i$  which is the output or correspond to the interleaved input data elements as shown in Figure 3.1. The input column vector  $X_i$  is multiplied to scrambling matrix to achieve interleaved sequence as:

$$Y_i = S \cdot X_i \quad (3.4)$$

More explicitly, (3.4) can also be written as:

$$\begin{bmatrix} Y3 \\ Y1 \\ Y4 \\ Y2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} X1 \\ X2 \\ X3 \\ X4 \end{bmatrix} \quad (3.5)$$

The above equation gives an overview of SBR scrambler used to scramble the input data elements. The details of generating scrambling matrix for SBR Interleaver will be discussed in next section.

### 3.3.2 Seed Based Random Scrambling (SBRS)

In order to design proposed SBR Interleaver, scrambling matrix is design. The scrambler makes use of random sequences uniquely generated by using an input seed to initialize proposed technique. The SBR Interleaver design method has inherent properties for optimal performance. The design allows one to use a unique random sequence. As mentioned earlier, this can be generated by using either a RAND function of MATLAB or by using chaotic logistic map (CLM). The design of SBRS with inherent properties leads to the optimal interleaving.

The design of proposed SBRS was first considered using RAND function of MATLAB®. The random sequences with RAND function can easily be generated with rand function. RAND function generates pseudo random numbers of given length. MATLAB® support three generator algorithms to generate random number. The syntax to use random generator is *RAND ('method', S)*. The random sequences are generated based on given 'method' in MATLAB®, and initialized by the state of the generator. Referencing MATLAB® the 'method' uses one of the following strings:

- 'State' uses a modified version of Marsaglia's Subtract-with-Borrow algorithm, the default in MATLAB® Versions 5 and later. The Subtract-with-Borrow is the variation of lagged- Fabonacci type. The parameter used in Marsaglia's algorithm happens to satisfy the prime number and primitive root



consition. The 'state' method can generate all the double precision values in the closed interval  $[2^{-53}, 1-2^{-53}]$ , and, theoretically, can generate over  $2^{1492}$  values before repeating itself.

- 'Seed' uses a multiplicative congruential algorithm, the default in MATLAB Version 4. This algorithm is basis for many random number generators. It uses three integer parameter and input seed to generate sequences. This method generates double precision values in the closed interval  $[1/(2^{31}-1), 1-1/(2^{31}-1)]$ , with a period of  $2^{31}-2$ .
- 'Twister' uses the Mersenne Twister algorithm by Nishimura and Matsumoto. Mersenne twister is a pseudo random number generator. It is based on a matrix linear recurrence over a finite binary field  $F_2$ . It provides for fast generation of very high-quality pseudorandom numbers, having been designed specifically to rectify many of the flaws found in older algorithms. This method generates double precision values in the closed interval  $[2^{-53}, 1-2^{-53}]$ , with a period of  $(2^{19937}-1)/2$ .

The varying sequences are generated using RAND based on internal state of the generator. MATLAB defines 32 different states, so setting the generator to different state leads to new sequence each time; however, it does not improve any statistical properties. Since, MATLAB resets the state at start-up, RAND generates the same sequences of number in each session unless the state is changed. For RAND function user defined seeds can be used to generate different random sequences within the given limits.

Other methods are also available to generate random sequences. One of the methods is to generate sequence using chaos. In our proposed scheme, the position of each input data element is substituted. In our proposed seed based scrambler the random numbers are also generated chaotically to generate interleaving patterns. The chaotic logistic map (CLM) is a well known 1-D map used to generate random number. As mentioned earlier that proposed design is not based on how good random sequence should be rather it is based on the inherent properties acquired by our proposed SBR Interleaver. Therefore,

random sequences using RAND function or generated using chaos does not give any extra benefits in the proposed SBR Interleaver to generate interleaving patterns.

In order to generate the random sequences using chaos, the logistic map is iterated with a unique initial condition – initial condition is served as a key and derived from external key. The external key is derived by the clients using 802.11i key management protocol.

Since the CLM is convenient to implement, we have selected it for demonstrating our scrambling algorithm. However, it should be mentioned that even other 1-D chaotic maps can be employed for scrambling purpose – maps which have uniform probability distribution functions such as piecewise linear chaotic maps.

The relative simplicity of the logistic map makes it an excellent point of entry into a consideration of the concept of chaos. CLM demonstrate how simple complex chaotic behavior can arise from very simple non- linear dynamical equation. The map was popularized in a seminar 1976 paper by the biologist “Robert May”, in part as a discrete-time demographic model analogous to the logistic equation first created by “Pierre François Verhulst” that is referenced from Wikipedia.

Mathematically the chaotic Logistic map is given by

$$x_{n+1} = rx_n(1 - x_n) \quad (3.6)$$

where  $0 < x_n < 1$  and  $3.47 < r < 4$ . The most attractive feature of logistic map is that it gives chaotic dynamics, when “ $r$ ” between 3.47 and 4.

After generating random sequences, these sequences are used by proposed scrambling algorithm. Based on the scrambling algorithm, discussed in later section, input data blocks of given size are scrambled. So changing the input seeds gives rise to different random sequences and proposed scrambler will produce optimal interleaving sequences at the output.



### 3.3.3 Initialization of SBRS

#### 3.3.3.1 Extracting unique initial condition from external key

In order to efficiently encrypt/decrypt the transmission data, same seed/key should be used by both transmitter and receiver to correctly recover the data. Therefore, same key should be derived at both sides. The key sharing of proposed SBRS uses same 802.11i key management protocol. In this proposed work, 128-bit key length is considered for derivation.

For proposed SBRS, the key is first derived based on random sequence generator function (RSGF). In this thesis, we used two RSGF namely as RAND function in MATLAB® and CLM. For simplicity, in the rest of the discussion we use RSGF as the seed based random sequence generator function. The initial condition seed/IC that is used to encrypt/ decrypt the input data elements for transmission is derived using 16 RSGF – each driving its own initial condition from the external secret key of 16 characters, and one master initial condition (MIC) that is used to select the generator function out of 16 RSGFs. Hence, no need to transfer extra key information to other side for decryption.

The secret key in ASCII form is denoted by

$$K = K_1 K_2 K_3 \cdots K_{16} \quad (3.7)$$

Here  $K_i$  denotes the 8-bit block of the secret key. Using  $K_i$ , the  $i^{th}$  initial condition  $IC_i$  is given by:

$$IC_i = \frac{K_i}{256} \quad (3.8)$$

The  $IC_i$  uniformly mapped to a value between (0, 1). For all 16-RSGF, one can find the  $IC$  as follows:

$$S \equiv \sum_{i=1}^{16} RSGF_i^{K_i}(IC_i) \quad (3.9)$$

$$IC = S \bmod 1 \quad (3.10)$$

where  $S$  refers to an intermediate variable and  $K_i$  to the number of the iteration of the  $i^{th}$  RSGF with corresponding initial condition  $IC_i$ . The MIC is derived from the secret key as follows

$$MIC = \frac{((K_1 + K_2 + K_3 + \dots + K_{16}) \bmod 256)}{256} \quad (3.11)$$

The MIC serves as initial condition to one RSGF from the bank of 16 RSGFs to initialize proposed SBRS.

### 3.3.4 Scrambling Algorithm

In a simple way, Scrambling is a technique to change the positions of data elements. In our proposed scheme, each data element is substituted. Our aim is to generate scrambling matrix,  $S$ , of size  $N \times N$  where  $N$  denotes the number of input data elements to be scrambled:

$$S = \{S_1, S_{i+1}, \dots, S_N\}^T \quad (3.12)$$

where ' $S$ ' denotes the scrambling matrix, and  $S_i$  in scrambling matrix is a row vector with  $N-1$  zeros and only one 1. The position of '1' in row vector  $S_i$  denotes the position of  $i^{th}$  input element after scrambling.

$$S_i(P_i) = 1 \quad (3.13)$$

where  $P_i$ , a position vector denotes the position of '1' in row vector  $S_i$ . The position vector  $P_i$  is generated by iterating chaotic logistic map.



The design of proposed scrambler is divided into several steps as given below:

**Step 1:**

Divide the output range  $[0.1, 0.9]$  into  $N$  equal length subintervals, where ' $N$ ' denotes the number of input data elements to be scrambled. Hence, during the iteration of function, the output of RSGF that occurs outside the considered range will be neglected.

**Step 2:**

Label each region sequentially from  $0, \dots, N$ . Let the length of each region be denoted by  $\Delta L$ . Now, let us denote the first region by  $R_0 = [0.1, \Delta L]$ , second region by  $R_1 = (0.1 + \Delta L, 0.1 + 2\Delta L]$ , 3<sup>rd</sup> region by  $R_2 = (0.1 + 2\Delta L, 0.1 + 3\Delta L]$ , and last region by  $R_N = (0.1 + N\Delta L - \Delta L, 0.1 + N\Delta L]$ . Now, label each region sequentially, i.e.,  $R_0 \rightarrow 0$ ,  $R_1 \rightarrow 1$ ,  $R_2 \rightarrow 2$ , and  $R_N \rightarrow N$ .

**Step 3:**

Iterate the RSGF using selected initial condition  $IC$ . RSGF is iterated until all the positions in position vector is filled as

$$P = \{P_i, P_{i+1}, \dots, P_N\} \quad (3.14)$$

where  $P$  denotes the position vector  $P_i$  and  $P_N$  signifies the position of ' $1$ ' in scrambling matrix. During the course of iteration, whenever RSGF falls in the specific subdomain, the number assign to that subdomain is stored in position vector  $P$ . If the function has already traversed the specific subdomain or interval, then the position corresponding to that subdomain is ignored. The iterations will continue until the function has traversed all the subdomains. For example  $[x_0, x_1, x_3, \dots, x_N]$  are the input elements may falls in the subintervals indexed as  $[P_4, P_5, P_3, P_2, \dots, P_1]$

**Step 4:**

Stop iterating the function, when it has finished traversing all regions.

**Step 5:**

Finally, the scrambling matrix  $S$  of size  $N \times N$  is generated by using position matrix generated by the above mentioned methodology. The complete scrambling matrix after assigning each position is written as

$$S_{i,k} = \begin{bmatrix} S_{i,k} & S_{i,k+1} & \cdots & S_{i,N} \\ S_{i+1,k} & S_{i+1,k+1} & \cdots & S_{i+1,N} \\ \vdots & \vdots & \ddots & \vdots \\ S_{N,k} & S_{N,k+1} & \cdots & S_{N,N} \end{bmatrix} \quad (3.15)$$

The above matrix can be written as

$$S = \{S_i, S_{i+1}, \cdots, S_N\}^T \quad (3.16)$$

where  $S_i$  is the row vector.

The algorithm works in such a way that each row vector in scrambling matrix contains "1" as

$$S_i \oplus S_j = 0, \quad i \neq j \quad (3.17)$$

where  $j$  is any other row vector of scrambling matrix  $S \in [i, N]$



### 3.3.5 Descrambling Algorithm

In SBRS, the descrambling/decryption consist of similar steps for both RSGF that includes chaos using CLM and RAND based function in MATLAB<sup>®</sup>. The position matrix and then scrambling matrix is derived in a same way as in the scrambling algorithm. In order to decrypt properly, key derivation at both transmitter and receiver should be same. Scrambling matrix is multiplied with scrambled data to restore all elements at the receiver end.

### 3.4 Performance Parameters - Spread and Dispersion

Random interleavers are basically analyzed based on their properties of spread and dispersion. These properties of 'spread' and 'dispersion' form the basic tool to examine the behavior of random interleavers. The performance of random interleaver is improved with careful selection of spread value and dispersion that comes with certain parameters used to generate random sequences and also based on inherent design criteria. The achieved value of spread given in literature for improved random interleaver and that converged in reasonable time is  $\sqrt{N/2}$ . The interleaver dispersion investigates the introduced regularity. Good value of dispersion assures that generated interleaving sequences have randomness in spread. Algebraic interleavers that are considered to be memory efficient and less complex, but do not have good value of dispersion and it is around neighboring of 0.5. The simulation parameters used to analyze and obtained results for both spread and dispersion are discussed as follows:

#### 3.4.1 Simulation model and parameters

In order to find out spread of proposed SBR Interleaver simulations, are carried out in MATLAB. Firstly, the input data of size  $N = 128, 256$  and  $512$  are send to proposed SBR interleaver to obtain scrambled position vector. Afterwards, the spread of proposed SBR Interleaver is calculated for all input combinations and interleaved output combination using the spread equation as follows:

$$|i - j| < S \text{ implies } |\pi(i) - \pi(j)| > S \quad (3.18)$$

where  $i$  and  $j$  are the input data elements before interleaving and  $\pi(i)$  and  $\pi(j)$  are the interleaved data elements, and  $\pi$  stands for interleaver. The minimum spread is "1" for random interleaver. The value of spread " $S$ " is varied from "2" and above to find out the achieved spread. The range of both input and interleaved sequences is [0.1 to 0.9]. The difference in the position of input elements before and after the interleaving process will give the values of spread. For each input elements pair that are one bit, two bits or more apart, interleaved distances will give the values of achieved spread.

Similarly, the dispersion of the proposed SBR Interleaver is found in the same manner as in spread, described hereafter. The input data of size  $N=128, 256$  and  $512$  are used by SBR Interleaver to generate interleaved position vector. The list of differences in input and output/interleaved pairs are computed using the following equation

$$D(\pi) = \{(j - i, \pi(j) - \pi(i)) | 0 \leq i < j < N\} \quad (3.19)$$

where " $N$ " is the total number of elements.

In order to find out the dispersion, all possible pairs using Equation 3.19 are generated as follows:

- Firstly, when the distance between input elements before interleaving is '1', '2' and so on till the  $N^{\text{th}}$  element, the corresponding distances of input elements after interleaving is calculated and tabulated in pairs.
- If any two pairs with same input distance before interleaving leads to same distances after interleaving, these cannot be entertained and only one pair is considered and remaining pair is discarded.
- The neglected pairs ' $q$ ' is also counted to find out the normalized value of dispersion.
- The normalized value of dispersion is calculated using the formula  $\frac{2|D(\pi)|}{q(q-1)}$ , where  $|D(\pi)|$  the total numbers of pairs and ' $q$ ' the total number of repeated pairs that will introduce regularity in the interleaving.



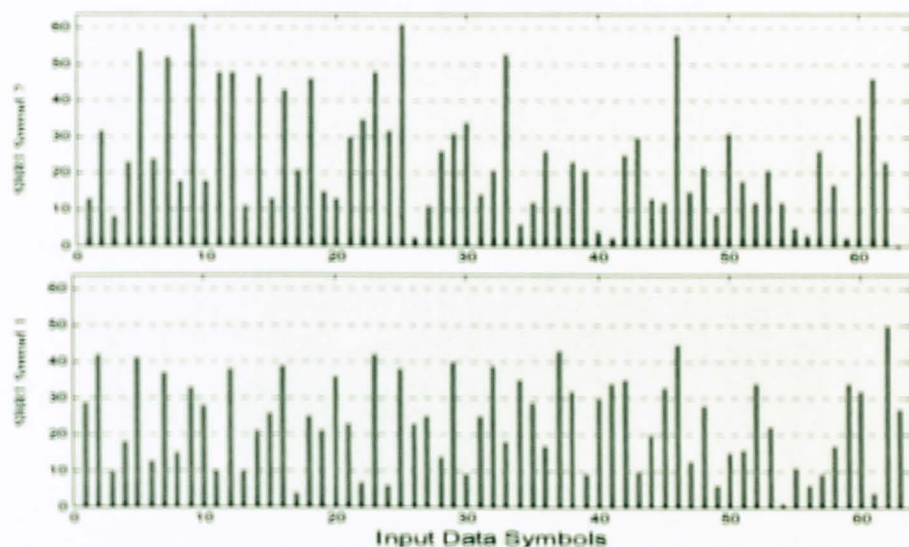


Figure 3.2: Achieved Spread of SBR Interleaver with  $S < 2$  and  $S < 3$

### 3.4.2 Results and Analysis

#### 3.4.2.1 Analysis of SBR Interleaver Spread

This section will discuss the results that have been obtained from previous chapter. The spread of SBR Interleaver is given in Figure 3.2 with  $S < 2$  and  $S < 3$ . The first plot shows the input elements that are one bit apart before interleaving and interleaved input elements with achieved spread. Second plot shows the input elements that are two bits apart before interleaving and achieved spread after applying proposed SBR Interleaver. The X-axis shows the locations of input elements and Y-axis shows the achieved spread. Our proposed SBR Interleaver efficiently interleaves the input elements with high spread. The histogram of achieved spread is given in Figure 3.3. The X-axis describes the number of input elements and Y-axis the achieved spread values and Z-axis shows the number of pairs.

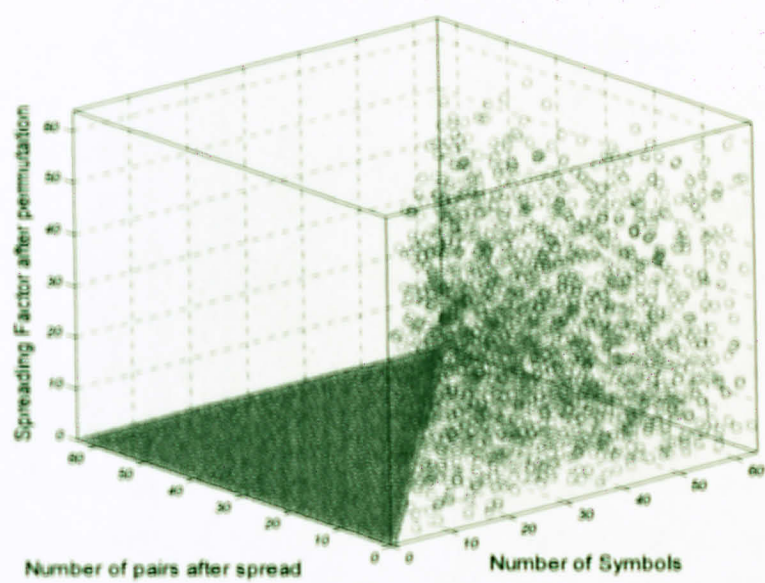


Figure 3.3: Histogram of SBR Interleaver Spread Pairs

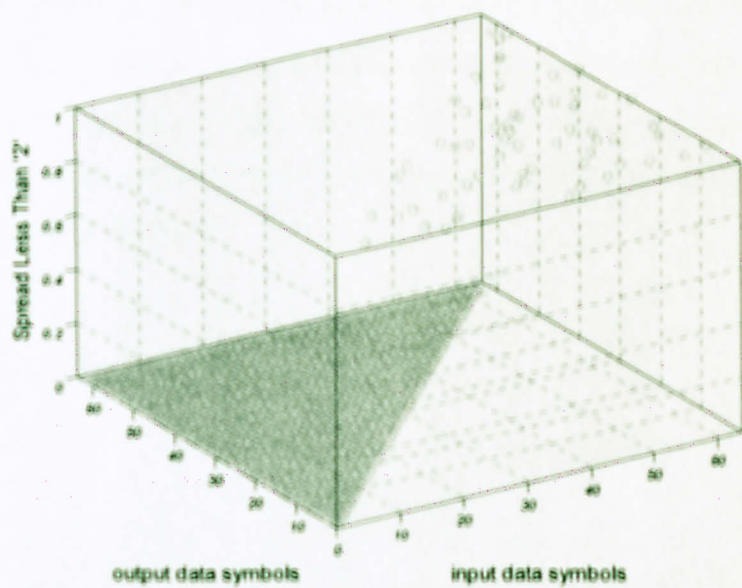


Figure 3.4: Histogram of low probability to generate spread  $S < 2$



The design of interleaver should have the property to inherently avoid the low spread elements and improves the performance of interleaver in burst error environment. Our proposed SBR Interleaver inherently introduces a mechanism to separate low spread input elements by dividing domain between [0.1-0.9] into equal  $N$  intervals and improves the performance by avoiding input data elements if it falls within the same interval again. Our proposed interleaver has inherent design to achieve good value of spread. Therefore, comparison of proposed SBR interleaver with both pseudo random sequences using RAND function and with chaotic sequences using CLM is carried out. The achieved minimum spread and average spread using chaotic sequences is tabulated in Table 3.1-3(a) and using MATLAB RAND function in Table 3.1-3(b). It shows that our proposed SBR interleaver has good value of spread and has same performance with both random sequences and performance of SBR interleaver does not depend on random source used to generate sequences. The average spread achieved with proposed SBR Interleaver is nearly  $N/2$  and more than 90% of input elements have spread  $S > \sqrt{N/2}$ . Moreover, it has very low probability to generate low spread values as shown in the Table 3.1 and depicted in Figure 3.4. The properties of random interleavers are discussed in [K. Xie et al. 2006][Y. B. Luis et al. 2004]. In all these interleavers, maximum possible spread try to achieve is  $\sqrt{N/2}$  and increasing the spread can improves the performance but on the cost of complexity. Our proposed SBR Interleaver can generate high spread values with reasonable complexity and also avoid storing positions each time as compared to spread or semi random interleavers.

Table 3.1(a): Chaotic SBR Spread with  $N=128$  and Spread  $\leq 2$ 

Input Seeds	Pairs Spread $\leq 2$	Minimum Spread	Average Spread
0.1242	2	01	44.4609
0.1950	2	01	45.5469
0.2241	2	01	44.4844
0.2833	1	01	42.7109
0.3125	1	01	43.6641
0.3921	1	01	46.4141
0.4381	1	01	40.9453
0.5291	2	01	43.7656
0.5923	1	01	47.5625
0.6237	1	01	44.0781
0.6927	0	01	48.7109
0.7433	1	01	42.8756
0.7866	0	01	42.4766
0.8112	0	01	45.4609
0.8998	2	01	43.0234
0.9026	1	01	43.3595
0.9533	0	01	46.9141



Table 3.1(b): RAND Based SBR Spread with  $N=128$  and Spread  $\leq 2$ 

Input Seeds	Pairs Spread $\leq 2$	Minimum Spread	Average Spread
0.1242	1	01	44.1016
0.1950	2	01	43.1328
0.2241	2	01	43.8043
0.2833	2	01	41.5000
0.3125	0	01	43.7422
0.3921	3	01	46.2031
0.4381	2	01	40.3906
0.5291	2	01	42.5313
0.5923	2	01	42.7656
0.6237	0	01	41.8750
0.6928	0	01	43.1643
0.7433	1	01	40.9141
0.7866	1	01	47.5010
0.8112	1	01	45.4766
0.8998	0	01	41.7344
0.9026	0	01	42.9766
0.9533	2	01	41.3672

Table 3.2(a): Chaotic SBR Spread with  $N=256$  and Spread  $\leq 3$ 

Input Seeds	Pairs Spread $\leq 3$	Minimum Spread	Average Spread
0.1242	02	01	89.3281
0.1951	03	01	90.7813
0.2245	03	01	87.7500
0.2844	03	01	88.9336
0.3125	03	01	91.4805
0.3921	02	01	91.2539
0.4381	02	01	85.9414
0.4954	02	01	88.3594
0.5295	02	01	90.0820
0.5923	01	01	90.6055
0.6357	02	01	88.0781
0.6927	03	01	86.0039
0.7431	01	01	88.1680
0.7879	02	01	88.3164
0.8102	03	01	90.7930
0.8999	02	01	89.5078
0.9026	04	01	93.2969
0.9531	04	01	92.7969



Table 3.2(b): RAND Based SBR Spread with  $N=256$  and Spread  $\leq 3$ 

Input Seeds	Pairs Spread $\leq 3$	Minimum Spread	Average Spread
0.1242	03	01	81.9453
0.1951	04	01	88.5820
0.2245	03	01	85.6016
0.2844	03	01	83.3516
0.3125	03	01	86.4102
0.3921	02	01	88.3125
0.4381	04	01	80.9688
0.4954	03	01	84.0352
0.5295	02	01	82.0859
0.5923	03	01	85.2734
0.6357	02	01	95.4492
0.6927	04	01	84.1875
0.7431	03	01	85.4606
0.7879	03	01	86.0039
0.8102	04	01	80.0547
0.8999	02	01	84.1367
0.9026	00	01	83.5781
0.9531	02	01	92.0273

Table 3.3(a): Chaotic SBR Interleaver Spread with  $N = 512$  and Spread  $\leq 4$ 

Input Seeds	Pairs Spread $\leq 4$	Minimum Spread	Average Spread
0.1242	04	01	177.5371
0.1951	03	01	179.0898
0.2245	02	01	179.5449
0.2844	03	01	182.8770
0.3125	04	01	182.3184
0.3921	04	01	180.9941
0.4381	03	01	173.4902
0.4954	04	01	176.5820
0.5295	04	01	173.5020
0.5923	04	01	178.7695
0.6357	04	01	183.0078
0.6927	03	01	183.0391
0.7431	02	01	179.9473
0.7879	04	01	187.6289
0.8102	04	01	187.9023
0.8999	04	01	178.6875
0.9026	03	01	182.2129
0.9531	05	01	173.9258

Table 3.3(b): RAND Based SBR Interleaver Spread with  $N=512$  and Spread  $\leq 4$

Input Seeds	Pairs Spread $\leq 4$	Minimum Spread	Average Spread
0.1242	05	01	171.2051
0.1951	03	01	180.3438
0.2254	01	01	171.8438
0.2844	05	01	168.0938
0.3125	04	01	175.2559
0.3921	04	01	173.5195
0.4381	05	01	183.7912
0.4954	03	01	168.9648
0.5295	04	01	175.4512
0.5923	06	01	169.3594
0.6385	04	01	185.8691
0.6927	03	01	171.6445
0.7431	05	01	174.1934
0.7879	04	01	174.0781
0.8122	02	01	174.5137
0.8999	04	01	175.7227
0.9026	03	01	171.1289
0.9531	06	01	171.3558



### 3.4.2.2 Analysis of SBR Interleaver Dispersion

The detailed discussion on interleaver spread and factors that improve the spread have also been analyzed. Randomly design interleavers have dispersion around 0.8. Most of the interleavers i.e., algebraically constructed interleavers have dispersion around 0.5. Algebraically constructed interleavers are application specific, and do not have good dispersion, but works reasonably good to meet the requirement of specific application.

Results are obtained to compare the performance of proposed SBR Interleaver dispersion using both random sequences. The obtained dispersion with both random sequences is tabulated in TABLE 3.4(a) and 3.4(b). Results are obtained with varying seeds and changing the size of interleaver. Our proposed SBR interleaver proved to have same dispersion using both random sequences. The dispersion is ranging from 0.80- 0.83, and varying input condition has not much difference in dispersion. Moreover, changing random sequences has no effect on the performance of SBR interleaver properties. The SBR Interleaver dispersion is also plotted against initial seeds with varying input sizes and is given in Figure 3.5. The X-axis shows the initial conditions to generate various interleaving patterns to obtain position vector and Y- axis shows the dispersion values. The plot shows three curves each for different input size and corresponding dispersion. It can be seen that proposed SBR Interleaver dispersion is above the 0.8 limit. Additionally, the size of interleaver has no effect on the dispersion of the interleaver. Our proposed SBR Interleaver will efficiently spread the input elements with very good randomness in interleaving. In order to visualize randomness, the histogram of SBR Interleaver dispersion is shown in Figure 3.6.

Table 3.4(a): SBR Dispersion with  $N=64, 128, 256$  with Chaotic Input Seeds

Input Seeds	SBR Interleaver DISPERSION		
	$N=64$	$N=128$	$N=256$
0.1135	0.8130	0.8167	0.8152
0.1923	0.8274	0.8130	0.8141
0.2234	0.8180	0.8169	0.8179
0.2877	0.8309	0.8092	0.8137
0.3259	0.8249	0.8137	0.8154
0.3921	0.8165	0.8206	0.8159
0.4381	0.8274	0.8073	0.8134
0.4854	0.8180	0.8162	0.8112
0.5295	0.8284	0.8212	0.8171
0.5923	0.8249	0.8194	0.8162
0.6357	0.8239	0.8134	0.8136
0.6937	0.8309	0.8147	0.8153
0.7431	0.8264	0.8241	0.8156
0.7879	0.8180	0.8124	0.8136
0.8192	0.8304	0.8129	0.8125
0.8999	0.8224	0.8051	0.8145
0.9026	0.8170	0.8182	0.8154
0.9531	0.8323	0.8123	0.8146

Table 3.4(b): SBR Dispersion with  $N= 64, 128, 256$  with Rand Function

Input Seeds	SBR Interleaver DISPERSION		
	$N=64$	$N=128$	$N=256$
0.1568	0.8328	0.8199	0.8134
0.8837	0.8229	0.8156	0.8128
0.3015	0.8145	0.8120	0.8136
0.1881	0.8065	0.8227	0.8150
0.2181	0.8105	0.8215	0.8196
0.9265	0.8239	0.8207	0.8151
0.8482	0.8125	0.8162	0.8115
0.5726	0.8234	0.8150	0.8142
0.3046	0.8061	0.8151	0.8136
0.4881	0.8214	0.8139	0.8135
0.0952	0.8189	0.8123	0.8141
0.0150	0.8190	0.8152	0.8113
0.0409	0.8235	0.8191	0.8131
0.0204	0.8075	0.8119	0.8163
0.8369	0.8264	0.8155	0.8158
0.2888	0.8150	0.8136	0.8126
0.1554	0.8120	0.8178	0.8184
0.3631	0.8175	0.8147	0.8130



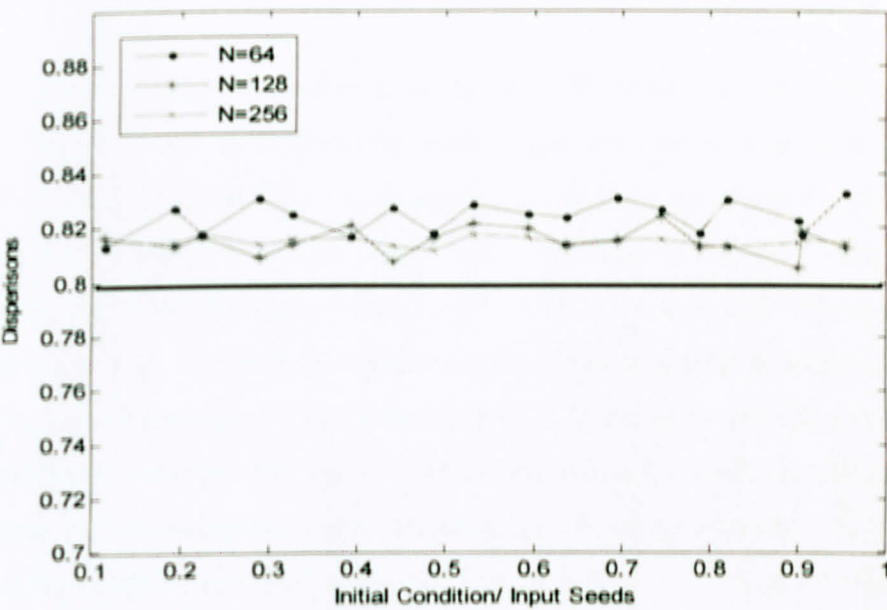


Figure 3.5: SBR Interleaver Dispersion with  $N= 64,128$  and  $256$

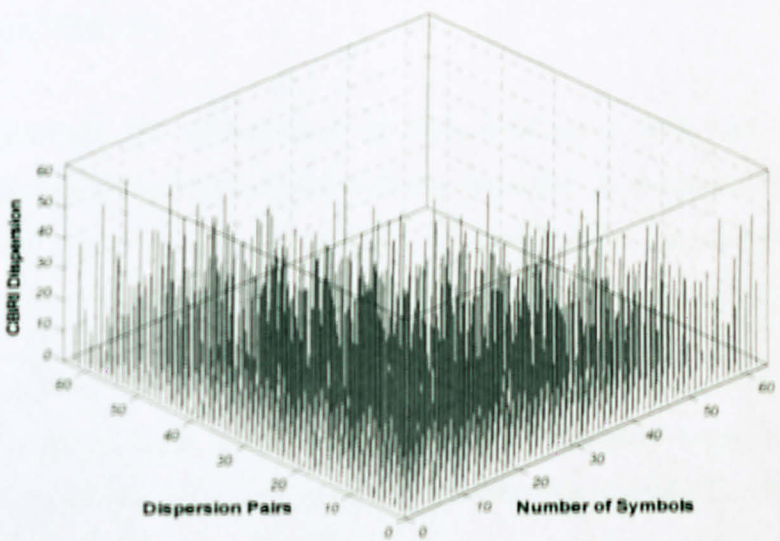


Figure 3.6: Histogram of SBR Interleaver Dispersion

### 3.5 Performance parameter - BER as Function of the Length of Burst Errors

The performance of the interleaver in terms of its bit error rate (BER) as a function of length of burst errors in conjunction with single error correcting code is evaluated hereafter for several cases. First experiment concerns the case where the performance of the proposed interleaver is compared with conventional random interleaver, now available as MATLAB function, called RANDINTRLV in terms of BER as a function of length of burst error. Secondly, the performance of the proposed interleaver is evaluated for two cases and compared – one when it is used in the conventional sense at bit level before modulation and another when it is used at symbol level after modulation. Thirdly, the performance of the interleaver is evaluated for OFDM system when the interleaver is used before and after constellation mapper. For its performance in an OFDM system, the WiMAX system is simulated in SIMULINK and the channel chosen are Stanford University's Interim (SUI) channels. Few representative values of Doppler are chosen to validate the performance.

#### 3.5.1 Comparison of SBR Interleaver with MATLAB's Random Interleaver (RANDINTRLV)

In order to compare the performance of SBR interleaver with MATLAB® random interleaver, sequences can be generated with any sequence. In the rest of the thesis results are carried out using one of the random sequences. For the comparison of SBR Interleaver and random interleaver, RAND function used to generate the sequences.

In order to interleave data using MATLAB random interleaver RANDINTRLV function is used. The inherent logic to generate interleaved sequences using RANDINTRLV function based on initials seeds to initialize given function and MATLAB RANDPERM function. RANDINTRLV uses RAND function to initialize random sequences later exploited by RANDPERM function that use its own seeding parameter with RAND function to generate permutation of given input data elements. After permuting input data elements using RANDPERM, default seed of RANDINTRLV function is restored for



further interleaving. RANDINTRLV function uses RAND function for both initializations of RANDINTRLV and RANDPERM functions. Later, based on RANDPERM, given sequences are interleaved.

#### **a) Simulation Parameters**

For simulations, 100 blocks of data of size  $N = 64, 128, 256, 512, 1024$  are taken. The data is encoded using linear block hamming binary code. The message to code length ratio is selected as (7, 4). Other available message to code length ratio can be selected with hamming distance of 3 so it can correct single error. When interleaver converts burst errors into single errors, this code is expected to work nicely and correct single error, if any, in given code length. However when interleaver is not able to convert burst into single errors, the error rate starts to increase. For encoding, any encoding scheme can be used and generator matrix is selected with any size that will correct single error. In MATLAB<sup>®</sup> various single error correcting codes are available with varying generator matrix sizes. For simplicity, in our analysis linear block hamming code is used. The coded data is interleaved using proposed SBR Interleaver and MATLAB<sup>®</sup> random interleaver, and then interleaved data passed through the modulator considering BPSK, QPSK, 4-QAM, 8-QAM, and 16-QAM. After performing modulation, signal is passed through AWGN channel. To evaluate the performance against burst errors- burst of errors are introduced manually. And, manually generated burst errors are XORed with modulated data. At receiver, bit error rate (BER) is calculated for proposed SBR Interleaver and also for random interleaver to compare the performance of both interleavers in burst errors environment.

#### **b) Results and discussions**

Our proposed SBR Interleaver has good properties of spread and dispersion. The random interleaver should be designed in such a way that it inherently improves the performance by converting maximum number of burst error into simple errors. This section will



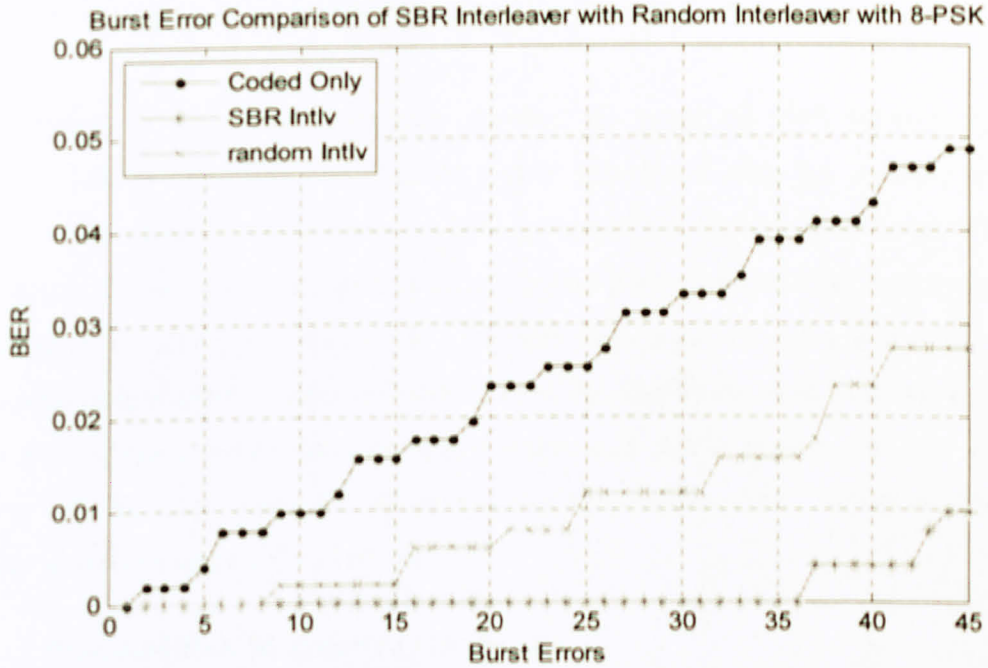


Figure 3.7: Burst Error Comparison of Proposed SBR Interleaver with Random Interleaver with 8-PSK and  $N=512$

analyze the performance of SBR Interleaver and MATLAB random interleaver against burst errors. The comparison of proposed SBR interleaver with MATLAB random interleaver is given in Figure 3.7. The 3 curves of BER represent coded data without interleaving, interleaved coded data with MATLAB random interleaver and proposed SBR interleaver. The X-axis shows the number of burst errors correction capability of interleavers and Y-axis the achieved BER of the interleavers. The plots show that our proposed SBR interleaver has the capability to correct long burst of errors as compared to MATLAB random interleaver. The correction of burst errors is due to inherent properties of interleaving. Moreover, randomly data is selected as input and interleaver randomly decorrelates the coded bits, so stair like curves are expected for BER values. It is seen from the results that proposed SBR interleaver can correct up to 40 bit long burst of data, while MATLAB random interleaver only correct 5 bits long burst of errors. The coding used can correct single random error in prescribed code length. The stair like BER curve for coded data without interleaver is due to hamming distance.

### 3.5.2 Introduction of SBR Interleaver in Typical Communication System

In a typical wireless communication system, our proposed SBR Interleaver can be replaced with conventional interleaver and is introduced after the channel coding to improve the system's performance in fading channel that causes burst errors. The block diagram of typical wireless communication system with proposed SBR Interleaver before modulation is shown in Figure 3.8. Only the transmitter blocks are shown in figure assuming that, at receiver side, the inverse of all the blocks are there to obtain transmitted data. As discussed earlier, interleaver is a simple and efficient method to deal with burst errors. The inherent properties of spread and dispersion of an interleaver lead to its unique performance in fading channel.

#### 3.5.2.1 Proposed Post Modulation Interleaver

The block diagram of proposed post modulation interleaver is shown in Figure 3.9. At post modulation, interleaving is performed on modulated data symbols. As mentioned earlier, in pre- modulation interleaver, interleaving is performed at bit level before modulation to facilitate channel coding. The size of the interleaver at pre- modulation is dependent on modulation scheme. Therefore, the complexity of interleaving is increased. The simulation parameters and to analyze the effectiveness of post modulation interleaver as compared to pre- modulation interleaver and its performance measures are discussed in the next section.

#### 3.5.2.2 Comparison of pre- modulation and Post modulation SBR Interleaver

Our study reveals that interleaver position can be changed. Therefore, interleaver is introduced after the modulation as shown in Figure 3.9. The simulation parameters analyze the proposed post modulation interleaver and for comparison, results of pre- and post modulation interleaver for possible advantages are described here.



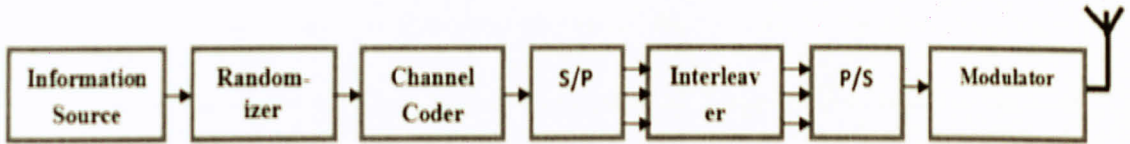


Figure 3.8: Block Diagram of Proposed Pre- modulation SBR Interleaver

#### a) Simulation Parameter

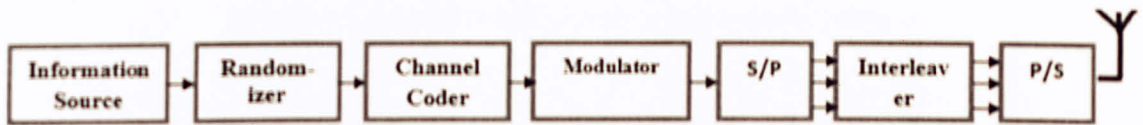
A complete typical communication system is taken into account to obtain results for pre-modulation and for post modulation interleaver. The proposed SBR Interleaver is also compared with random interleaver at post modulation position. For simulation, same parameters are used as discussed in section 3.5.1. First considering pre- modulation results, coded data is interleaved using proposed SBRs, and then interleaved data passed through the modulator. At receiver end, Bit Error Rate (BER) is calculated for proposed SBR pre- modulation Interleaver.

In order to obtain BER of proposed SBR Interleaver at post modulation interleaver, small change has to be introduced. After the channel coding and modulation, interleaving is performed on modulated data. The rest of the steps will remain same.

#### b) Results and Analysis

The comparison of proposed SBR pre- modulation interleaver with post modulation interleaver is given in Figure 3.10. For comparison, results are taken at both before modulation and after modulation positions. The 3 curves of BER in pre- modulation interleaver and post modulation interleaver Figures represents coded data without interleaving, interleaved coded data with MATLAB random interleaver and proposed SBR interleaver. The X-axis shows the number of burst errors correction capability of interleavers and Y-axis the achieved BER of the interleavers. To compare the performance, the burst of errors are introduced manually.





3.9: Block Diagram of Proposed SBR Post Modulation Interleaver

The study of pre- and post modulation interleaver has been analyzed and come up with the following points as given below:

- Interleaver position can be changed without affecting the performance of the system.
- In pre- modulation interleaving, only bit level processing/design is feasible. The size of interleaver changes the modulation scheme and also changes the coded bits per OFDM symbol.
- Interleaving complexity is increased with the choice of modulation because, at bit level, the size of interleaver is proportional to modulation scheme.
- In post modulation or symbol level processing, interleaving is performed on modulated data or constellation symbols.
- Symbol level interleaving has no effect on the energy of the modulation scheme used because each constellation symbol is again a regular constellation point.
- Symbol level interleaving has been considered a simpler design, because interleaving is performed after the modulation and interleaving is not dependent on modulation parameters.
- Finally, with post modulation interleaving, the size of interleaver is minimized. It implies minimum interleaving complexity.

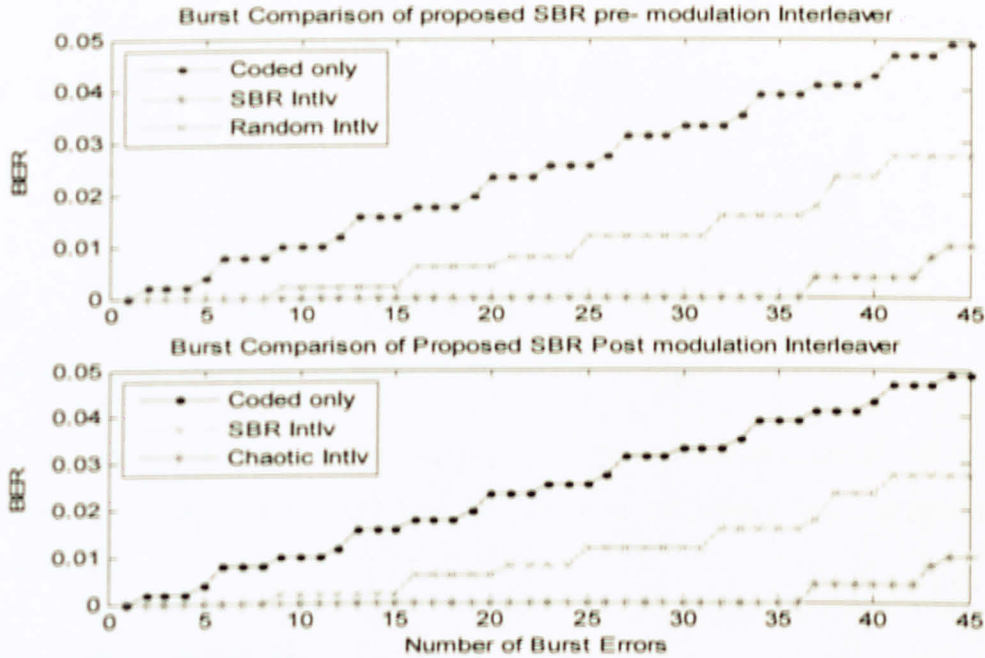


Figure 3.10: Comparison of proposed pre- modulation and post modulation Interleaver with 8-PSK

### 3.5.3 Introduction of SBR Interleaver in OFDM System - Before and After Constellation Mapper

Our proposed SBR Interleaver can also be extended and introduced in OFDM system. The proposed pre- modulation interleaver and post modulation interleaver is shown in the Figure 3.11. For OFDM based system, proposed SBR Interleaver is exploited as an interleaver before and after the modulation. In OFDM system, interleaving is performed after the channel coding. For pre- modulation interleaver, our proposed SBR Interleaver replaces the typical interleaver used in OFDM system and rest will follow the same for the simulation. However, for post modulation interleaver randomly generated symbols and serial to parallel conversion symbols are interleaved using proposed SBR Interleaver. The scrambling matrix of same size as input data symbols is generated as follows:

$$X_e = X_N \times S \quad (3.20)$$

where,  $X_N, S$  are the input symbols and scrambling matrix of size  $N \times 1$  and  $N \times N$  respectively. We obtain the OFDM baseband signal by applying the IFFT,

$$X_n = IFFT\{X_e\} \quad (3.21)$$

where,  $X_n$  is the frequency domain vector signal respectively. At receiver same procedure is followed to descramble the constellation symbols.

For the suitability of proposed pre- and post modulation interleaver in OFDM system, the simulation parameters to compare both pre- and post modulation interleaver is discussed in next section.

#### a) Simulation Parameters

For the implementation of proposed SBR Interleaver, OFDM system is considered and simulation is carried out in MATLAB. The pre- and post modulation interleavers are shown in Figure 3.11. The suitability and performance of pre- and post modulation interleaver is measured in SUI fading channel. The detailed description of each SUI channel has been given in [M. Driberg, 2005]. The selective values of Doppler are used as given in standard SUI channel model. In a fading environment, the received signal power varies randomly over distance or time due to multipath fading. There are different performance parameter used based on rate of change of fading. To analyze the performance of proposed pre- and post modulation interleaver, average bit error rate (BER) carried out as a function of signal to noise ratio (SNR). The Low values of SNR correspond to large error bursts. The average BER as function of SNR can be considered as performance parameter when signals fade is over few simultaneous symbols time, so deep fade will affect many simultaneous symbols in error. The pre- modulation follows the standard system with interleaving the coded data, modulation and then transmitted. However, for post modulation interleaver, interleaving is performed at the last before adding the cyclic prefix and after the modulation. Therefore, size of interleaver do not



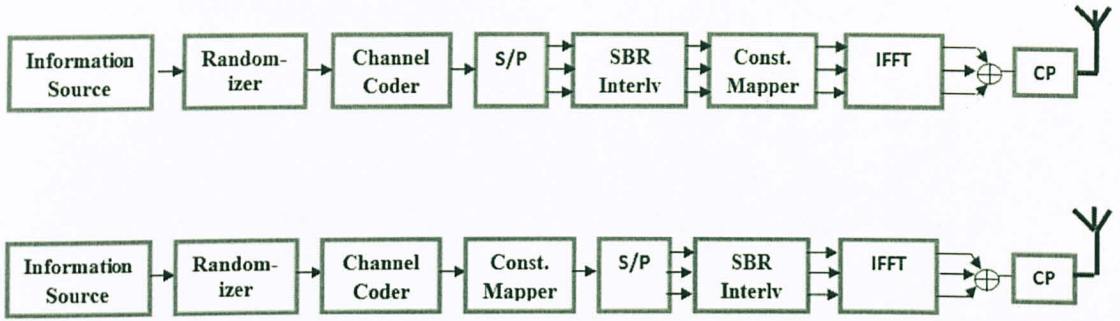


Figure 3.11: Block Diagram of Proposed OFDM System with SBR Pre- and Post Modulation Interleaver

depend upon the modulation scheme and has constant size. For the simulation, parameters are selected WiMAX standard (802.16d 2004) system and tabulated in Tables 3.5 to 3.8. There include 6 different burst profiles and four of these profiles have been used to obtain the results. The burst profile specify the modulation and forward error correction (FEC) used. The modulation and coded bits per OFDM symbol given in Table 3.6 is not considered for post modulation interleaver, because the size of modulation data is constant (192 symbols). After that, adding the cyclic prefix and IFFT are performed and then signal is passed through the channel. The channel is modeled by the 6 SUI channels with Additive White Gaussian Noise (AWGN). SUI channels are group of 6 channels used to evaluate air interface performance [Erceg et al, 2003]. The burst of error through SUI channels, default values of Doppler that has been given in standard SUI channel model is used. The 6 SUI channels model the typical channels for 3 types of terrains. Terrain type A is hilly terrain with moderate to heavy tree densities while terrain type C is flat terrain with light tree densities. Terrain type B is intermediate between terrain A and terrain C. Table 3.7 shows the terrain type and corresponding SUI channels that represent them. At receiver, BER of both pre and post modulation is obtained and compared for analysis.

Table 3.5: Specifications of 6 Burst Profiles

Burst Profile	Uncoded Block size (Bytes)	Coded Block Size (Bytes)	RS Code	CC Code Rate	Overall Coding Rate
QPSK with RS-CC rate $\frac{1}{2}$	24	48	(32,24,4)	2/3	$\frac{1}{2}$
QPSK with RS-CC rate $\frac{3}{4}$	36	48	(40,36,2)	5/6	$\frac{3}{4}$
16-QAM with RS-CC rate $\frac{1}{2}$	48	96	(64,48,8)	2/3	$\frac{1}{2}$
16-QAM with RS-CC rate $\frac{3}{4}$	72	96	(80,72,4)	5/6	$\frac{3}{4}$
64-QAM with RS-CC rate $\frac{1}{2}$	96	144	(108,96,6)	$\frac{3}{4}$	2/3
64-QAM with RS-CC rate $\frac{3}{4}$	108	144	(120,108,6)	5/6	$\frac{3}{4}$

Table 3.6: Number of Coded Bits per OFDM Symbol

Modulation	Coded Bits per OFDM Symbol ( $N_{cbps}$ )
QPSK	384
16- QAM	768
64 QAM	1152

Table 3.7: Terrain Type and Corresponding Sui Channels

Terrain Type	SUI channels
C	SUI-1,SUI-2 <sup>1</sup>
B	SUI-3, SUI-4*
A	SUI-5, SUI-6*

Table 3.8: General Characteristics of Sui Channels

K-Factor : Low			
Doppler	Low Delay Spread	Moderate Delay Spread	High Delay Spread
Low	SUI-3		SUI-5
High		SUI-4	SUI-6
K-Factor : High			
Doppler	Low Delay Spread	Moderate Delay Spread	High Delay Spread
Low	SUI-1 ,SUI-2		
High			

<sup>1</sup> SUI- 1 and SUI-2 belong to the same terrain but have slightly different specifications like doppler, delay and power.

\* Same is true for SUI- 3& SUI-4 and SUI-5 & SUI-6.



**b) Results and Analysis**

The comparison of pre- and post modulation interleaver has been done to show the feasibility and effectiveness of changing the position in terms of complexity and performance of the system in OFDM system. The average BER is plotted verses SNR to evaluate the performance and to examine the suitability of interleaver before and after the constellation symbols. The results have been obtained for all 4 mandatory profiles and all 6 SUI channels with  $1 \times 1$  Single Input Single Output (SISO) configuration. A  $1 \times 1$  SISO system with a channel that has been modeled as a 3 tap SUI channel followed by AWGN. The BER verses SNR plots with SUI channels is shown in Figures 3.12 and 3.13. The results are carried out with all SUI channels but half the results are reported here. The results show that changing the position of interleaver does not affect the performance of the system. The plots for BER are same for both configurations. Hence, if necessary interleaving can be done at bit level after the channel coding or interleaving can be done after the modulation. The possible advantages of pre- and post modulation interleaver that has been discussed earlier also hold for OFDM based system.

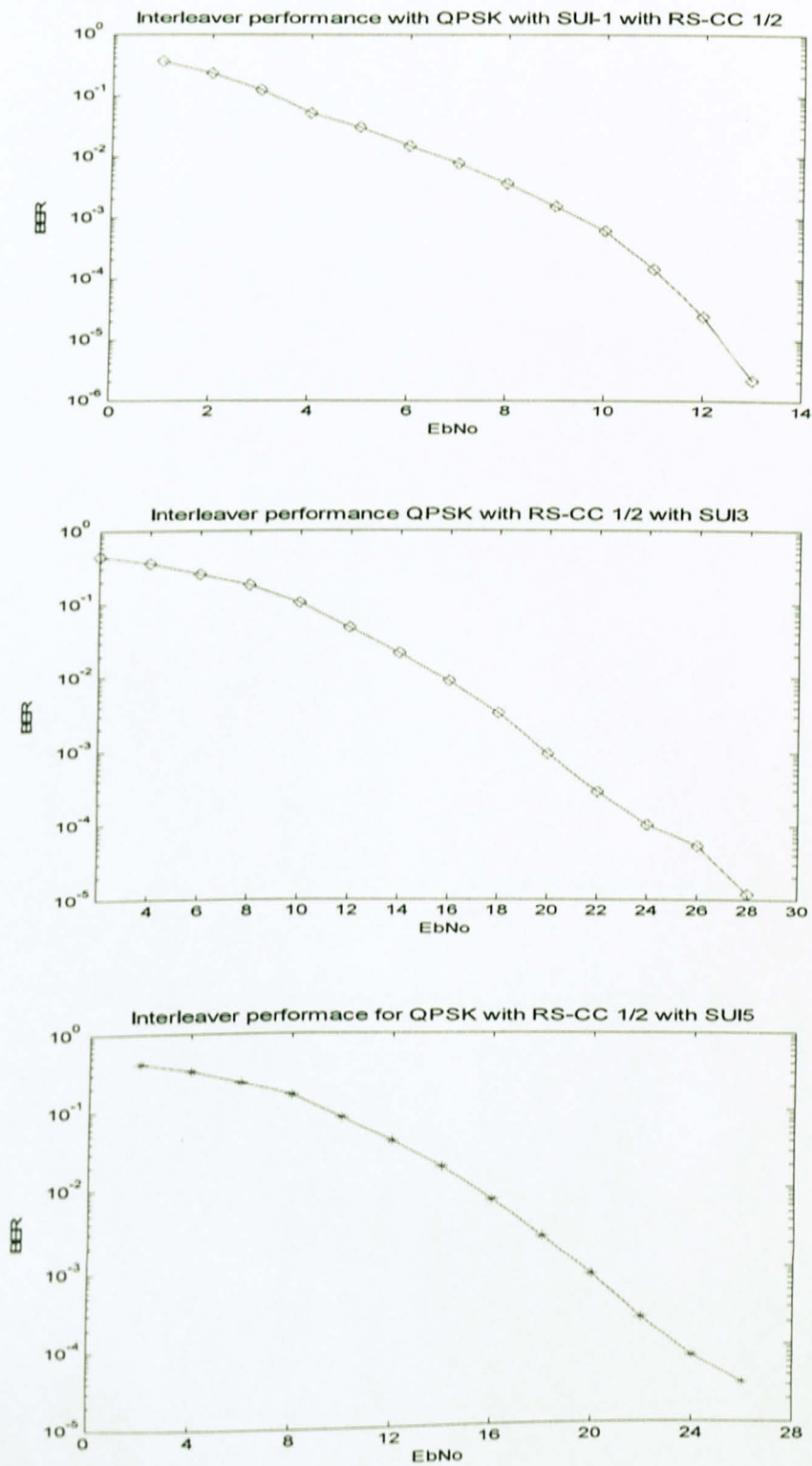


Figure 3.12: Pre- modulation Interleaver Performance for QPSK with RS-CC  $\frac{1}{2}$  and SUI- 1, 3, 5

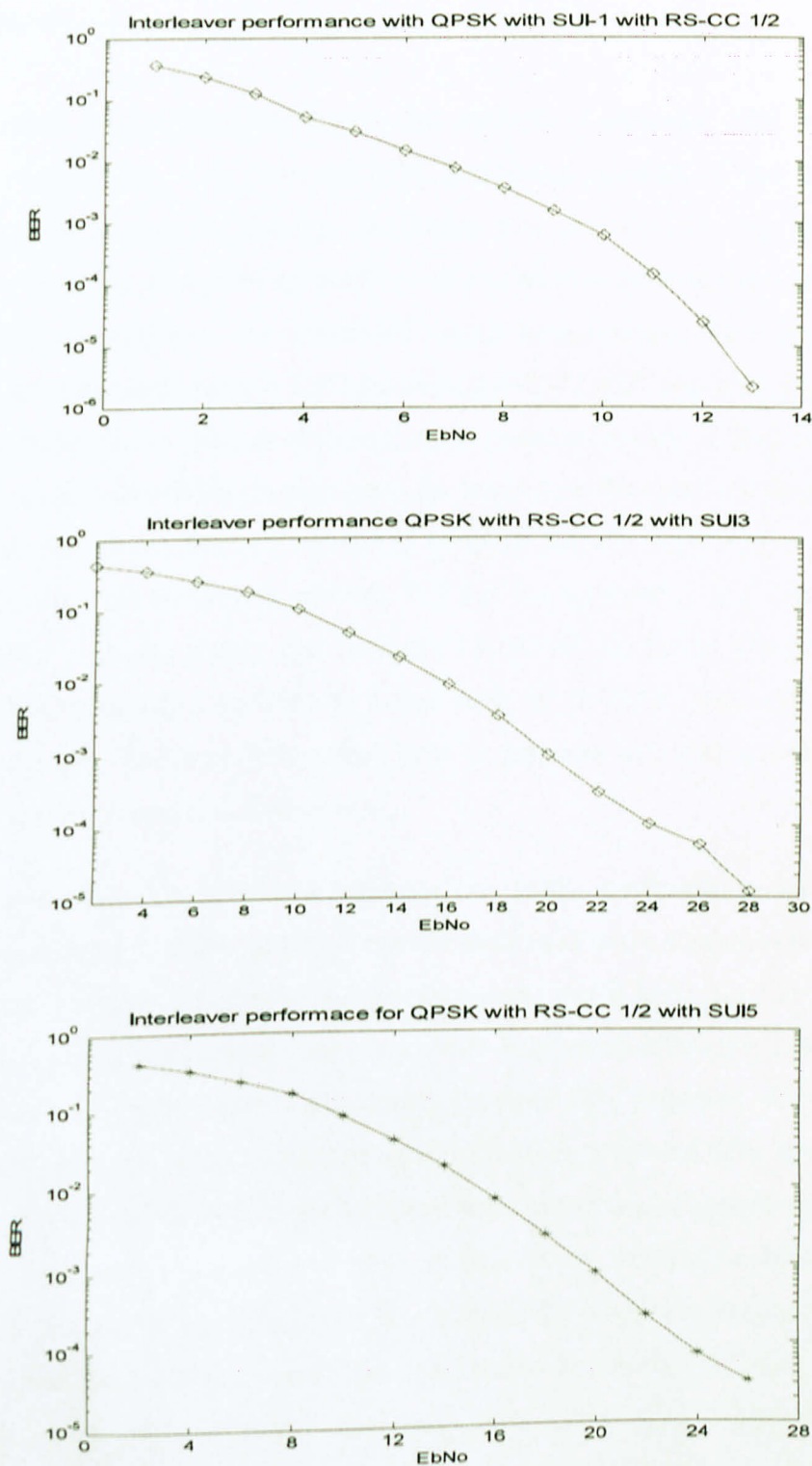


Figure 3.13: Post- modulation Interleaver Performance for QPSK with RS-CC  $\frac{1}{2}$  and SUI- 1, 3, 5



### 3.6 Summary

In this chapter, we described the design and analysis of proposed SBR Interleaver for improved performance. Our proposed SBR Interleaver consists of two main building blocks. First is to generate random sequences that are used by our proposed SBR Interleaver. Secondly, design of scrambling matrix that uses these random sequences. The unique random sequences are generated using two sources. The pseudo random sequences are generated using RAND function in MATLAB® and also generated using chaos with CLM. The purpose is to show that the proposed design of SBR Interleaver has inherent properties to efficiently interleave the input data elements and does not depend on the input random sequences. In order to initialize random sequences in our proposed SBR Interleaver, first the key is derived. The key for scrambling and de-scrambling is extracted from a stream cipher that employs 16- RSGF for Initial Condition and one RSGF for Master Initial Condition to select bank of 16-RSGF that will generate the scrambling matrix. The scrambling algorithm to generate scrambling matrix for SBR Interleaver is also presented and discussed.

The proposed SBR interleaver is analyzed to fulfill performance measures. The simulation parameter to carried out results and obtain results are discussed in this chapter. The comparison of SBR Interleaver using both chaotic and RAND function sequences is discussed first and it is shown that proposed SBR Interleaver efficiently interleave input data elements with both random sequences. Additionally, proposed design does not depend on the random sequences that are used to initialize proposed SBR Interleaver. It is shown that proposed SBR Interleaver has very good properties of spread and dispersion. The optimal interleaving properties of SBR Interleaver are inherent in design. The SBR Interleaver is designed in such a way that it will optimally interleave the input data and do not dependent on the random sources. The comparison of random interleaving properties proved that both sequences lead to the same good interleaving properties. First, the probability to generate low spread value while changing the size of the interleaver has been analyzed. Our proposed interleaver interleaves the input data elements so that, it has very low probability to generate minimum values of spread and changing the size of the

interleaver does not affect its performance. It is also shown that SBR Interleaver has very good dispersion property. The size of the interleaver has no affect on the dispersion of proposed interleaver. In order to optimize the size and performance of the system, SBR Interleaver is also analyzed by changing the position and it is introduced after the modulation in typical communication system and also for OFDM based system. As a result, changing interleaver position does not affect the performance of the system, but it can be helpful to decrease the complexity to interleave coded bits. Finally, proposed interleaver is compared with MATLAB random interleaver to analyze burst error correction capability. It is shown that proposed interleaver has the capability to correct long burst of errors as compared to MATLAB random interleaver. Additionally, both pre- and post modulation interleavers are also analyzed to correct burst error and have the same performance.



## Chapter

# 4

## SBR Interleaver as a PHY Layer Security Device

In Chapter 3, the design and analysis of proposed seed based random interleaver is discussed. Our proposed design has inherent properties to scramble the input data sequence and that leads to optimal interleaving properties with any random source. Therefore, in this work random sequences are generated using two sources. Pseudo random sequences are generated using RAND function in MATLAB<sup>®</sup> and chaotic sequences are generated using chaotic logistic map (CLM). The simulation parameter has been discussed to analyze the proposed SBR Interleaver. The analysis of proposed SBR Interleaver to improve the performance of wireless communication system in fading channel that introduce burst errors has been described. The analysis of random interleaving properties has been discussed. The suitability of SBR Interleaver at bit level before modulation and at symbol level when it introduce after the modulation for typical communication system and also for OFDM system in burst error environment has been given. The comparison of interleaver ‘spread’ and ‘dispersion’ with random interleaver given in MATLAB<sup>®</sup> has been made.

This chapter discusses the suitability of proposed SBR Interleaver as a PHY layer security to combat security attacks. The security of any system solely depends on encryption key and its performance is measured in terms of it strength to prevent security attacks on wireless communication system. In order to analyze the suitability of SBR Interleaver, key sensitivity analysis is carried out. To analyze the effectiveness



of key sensitivity analysis, various security attacks and their effectiveness is discussed.

#### 4.1 Introduction

Seed based interleaving patterns can be introduced as a PHY Layer security device. The property of the interleaver to generate seed dependent varying sequences to interleave the coded data can be used as a security mechanism. The transmitter uses a specific interleaving pattern owing to certain seed now called a key. If the receiver has the a-priori knowledge of the seed passed on to it by one of the several standard ways provided in, say, IEEE 802.11i framework, the receiver can generate the said interleaving pattern easily and therefore decode and deinterleave the data sent. Hence, input seeds that are used to initialize interleaving methods can be served as a key. To strengthen the security of interleaver design, generated sequences should not reveal any information that expose the key or input sequence. To make these possible, interleaving methods should be designed in such a way that it generates unpredictable scrambled sequence. The precise choice of interleaver to encrypt the transmission data will significantly strengthen the security of data. In wireless communication system, interleaver as a PHY layer security device comes at no extra cost in terms of system resources and it will help to further improve the security of PHY layer data.

Wireless LANs are highly susceptible to numerous malicious attacks. In wireless system layer abstraction is a very important concept, requiring each layer to provide independent functionality to strengthen the security of the system. At link layer and higher layers, security mechanisms are used to protect the transmission data to prevent attacker that manipulates useful information. Even if the strong confidentiality and mutual authentication protocols are used at MAC layer, it still leaves many weak spots for attacker to explore. At MAC layer only data frames are encrypted while leaving management and control frames unprotected. In addition, MAC headers are also left unencrypted. This unprotected information gives a chance for eavesdropper to sneak in and disrupts wireless transmission. The detailed of various malicious attacks on WLAN has been given and to some extent discussed in chapter 2.

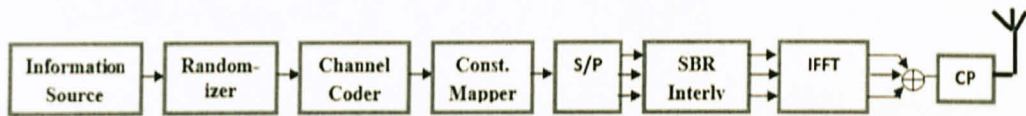


Figure 4.1: Block diagram of proposed SBR Interleaver as a PHY layer security device for OFDM system

The block diagram of proposed SBR Interleaver for OFDM system is shown in the Figure 4.1. Our proposed interleaver is introduced at PHY layer to interleave constellation symbols. Previously, encryption is made function of MAC layer. Therefore, encryption is applied only at bits stream level and to protect only data frames. The services running or building block of PHY layer includes coding, interleaving patterns and modulation schemes which are kept unprotected for the purpose to recover the transmitted information correctly at receiver as seen from the Figure 4.1. The unprotected PHY layer information and patterns like interleaving, modulation and coding is an open invitation for an attacker to sneak in the system. The interleaving, coding and modulation patterns can be kept secure for extra level of security. The proposed interleaver introduced after constellation symbols helps to protect PHY layer data. All services running on PHY layer will be protected because attacker has only waveform information to guess for any clue. An attacker has to break the introduced secure interleaving introduced at PHY layer to sneak in for bit level information for further analysis to break data confidentiality protocol.

In the following subsection, it is shown that by providing the security at the physical layer with proposed SBR Interleaver which scrambles the complete MPDU (MAC Protocol Data Unit) frame, Wireless LAN can be made secure against some of the current prevailing threats.

## 4.2 Performance Parameter- Key Sensitivity Analysis

Since a cryptosystem cannot exist without a key, it must be clearly defined what parameters serve as a key. Once the key has been defined, it is equally important to analyze the strength of the key in depth.



### **a) Simulation Parameters**

In order to perform key sensitivity analysis of proposed SBRS performed in MATLAB®, the symbols are randomly generated using MATLAB RANDINT function, and scrambled with proposed SBR Interleaver. For modulation QPSK, 4-QAM and 8-QAM for  $N=64$ , 128 and 256 carrier for 1000 OFDM frames are considered.

The constellation symbols are scrambled with proposed SBRS. At receiver end, the scrambled data is recovered back with the same scrambling matrix. After that, all the parameters are again used, but this time slightly different initial condition is used to generate the scrambling matrix. The purpose is to investigate the performance of proposed SBR Interleaver, and the probability to generate different position vector with given initial condition. The chosen initial condition slightly differs to analyze the sensitivity of initial condition to make decoding of scrambled data infeasible at the receiver end.

Our proposed SBR Interleaver can generate unique unpredictable sequences. With a small change in input seed will lead to completely different interleaving patterns. Therefore, the proposed SBR Interleaver is analyzed using both random sequences.

### **b) Results and Analysis**

The proposed OFDM system where SBR Interleaver is applied after modulation has been discussed in chapter 3. To analyze the key sensitivity, constellation symbols are scrambled with proposed SBR Interleaver, while scrambling matrix is generated using selected initial condition. At receiver, when descrambled with same initial condition, all constellation symbols are recovered with zero error. However, when the same data is recovered with slightly different initial conditions, almost all the constellation symbols are in error. The probability of error is uniformly distributed in symbols. The probability of occurrence of each constellation symbols when decrypted with slightly different initial condition is shown in Figure. 4.2. The X-axis presents the QPSK constellation symbols and Y-axis shows the probability of frequency of occurrence of each constellation symbol. The number of differing positions in the two scrambling



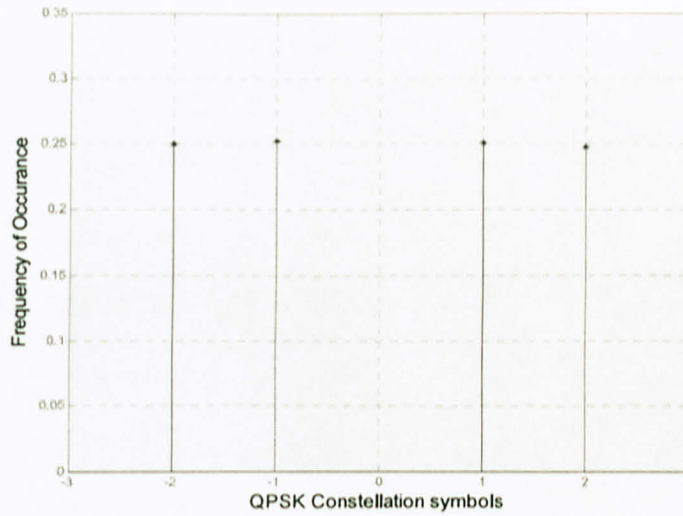


Figure 4.2: Probability of occurrence of constellation points with slightly different initial condition

matrixes generated with the two slightly different initial conditions is almost 99%. To show how efficiently our proposed technique will generate difference position with slightly change in initial condition is tabulated in Table 4.1 and initial conditions differ only 4<sup>th</sup> decimal digit. The generation of difference positions is not dependent on random sequences used to initialize proposed SBR Interleaver, rather it depends on inherent properties of proposed scrambler. To show that proposed technique has inherent properties and not dependent on random source, probability of error of differencing position also carried out using RAND function tabulated in Table 4.2 and results show that both sequences have nearly same performance. The slight change in initial condition can be selected for forward sequence or backward sequence. Our proposed SBR interleaver has same performance with both selection of slight change in initial condition. In order to show efficiency of generating scrambling sequences of proposed technique, sequences are generated and tabulated in Table 4.3. It shows that the input elements that are scrambled with slightly different initial conditions have different position vectors. Further, small variation in initial condition generates positions that lead to completely different trajectories. As the number of the input increases it will generate more random positions with slight difference in initial conditions. It confirms that with the slightly different initial condition it is infeasible to recover the data.

Table 4.1: Probability of Wrong Input Elements with Diff. Key using Chaotic Sequence

IC with Slight Diff.	Diff Position/512	%age Diff. position
0.1534,0.1535	511	99.80
0.2411,0.2412	508	99.21
0.3855,0.3856	510	99.60
0.4882,0.4883	508	99.21
0.5371,0.5372	512	100.00
0.6981,0.6982	509	99.67
0.7191,0.7192	511	99.80
0.8323,0.8324	510	99.60
0.9167,0.9168	511	99.80

Table 4.2: Probability of Wrong Input Element with Diff. Key using RAND function

IC with Slight Diff.	Diff Position/512	Percentage Diff. position
0.1534,0.1535	511	99.80
0.2411,0.2412	509	99.41
0.3855,0.3856	511	99.80
0.4882,0.4883	510	99.60
0.5371,0.5372	511	99.80
0.6981,0.6982	511	99.80
0.7191,0.7192	511	99.80
0.8323,0.8324	511	99.80
0.9167,0.9168	512	100.00

Table 4.3: Position Vector Generation with Slight Change in Initial Condition

Generated Positions With Proposed SBRS with Slight Change In Initials Condition											
0.1545	0.1546	0.2234	0.2235	0.4967	0.4968	0.5583	0.5584	0.6133	0.6134	0.7203	0.7204
34	34	48	48	6	5	9	9	8	8	57	57
2	3	60	63	37	35	44	44	43	43	43	43
27	28	33	33	9	14	18	18	12	12	11	12
12	7	3	4	45	55	62	62	51	52	50	51
51	41	28	1	64	48	30	28	55	54	44	56
54	6	8	22	23	61	17	11	48	50	15	45
48	37	42	12	11	31	60	49	60	57	58	20
60	10	44	51	49	10	35	60	33	42	40	64
35	46	15	55	59	32	16	36	3	9	3	22
10	63	58	47	38	17	58	2	28	44	30	13
47	27	41	62	15	60	40	25	7	17	8	54
61	17	5	28	56	9	2	27	39	61	14	49
31	61	36	10	44	44	27	50	1	33	55	58
3	33	2	46	16	19	45	56	21	20	46	40
29	8	26	63	58	63	20	16	15	19	63	2
21	42	1	27	39	27	21	59	57	64	27	27
16	9	24	16	1	16	8	37	41	24	17	53
59	45	23	59	8	59	43	8	42	7	60	55
38	64	9	38	43	36	15	43	44	41	34	47
18	22	45	13	13	2	56	13	16	6	5	62
14	14	21	53	54	12	59	54	58	38	1	28
11	56	18	34	14	51	36	57	40	60	22	5
49	21	61	15	46	34	3	58	2	34	12	34
58	16	31	57	24	3	28	40	27	5	51	3
40	59	29	42	5	28	13	4	56	35	47	30
28	36	19	9	35	33	53	33	46	36	62	6
9	48	63	64	12	11	52	6	64	63	29	39
44	60	27	23	51	49	51	38	23	25	4	19
17	5	17	44	60	37	46	15	10	2	33	24
33	2	32	17	36	8	63	53	47	27	49	7
5	25	22	61	20	42	25	51	62	51	36	4
55	29	11	31	19	46	4	45	6	56	20	33
62	1	50	11	63	64	33	21	37	45	64	31
7	24	57	49	25	24	14	17	63	21	23	59
39	23	43	58	3	52	55	35	26	18	24	38
1	11	62	39	28	54	48	10	20	62	35	14
24	50	7	21	7	50	34	46	19	28	10	29
6	58	40	18	41	57	19	63	9	10	61	18
23	40	64	29	18	41	26	14	59	48	13	61
45	19	10	3	62	7	32	55	24	23	53	26



64	26	46	8	29	4	54	47	36	3	48	1
22	12	14	43	40	39	49	29	25	11	32	23
56	51	55	52	2	26	38	52	22	49	52	8
30	30	47	54	27	1	57	41	13	58	54	11
50	52	6	37	53	6	42	7	54	39	59	50
36	53	37	6	21	45	10	3	50	1	39	42
4	44	35	50	30	20	29	30	4	22	19	10
8	43	34	41	42	22	31	39	31	14	42	48
42	13	25	2	17	15	6	32	29	29	9	21
15	54	13	25	34	56	11	42	30	30	45	17
57	57	53	32	52	21	39	61	11	46	25	60
43	4	52	36	50	58	1	31	5	26	28	52
41	31	54	45	4	40	23	19	34	15	6	63
26	55	49	26	33	43	61	64	17	4	37	25
20	32	59	19	55	47	7	24	61	32	38	15
13	38	38	24	48	29	5	34	32	37	16	44
37	15	56	56	61	25	50	48	38	40	7	41
32	49	12	14	32	30	41	5	35	31	2	37
52	39	30	7	22	53	37	20	52	16	18	36
53	20	16	40	57	23	12	23	14	59	31	35
46	18	39	30	47	13	24	12	45	47	26	16
63	62	4	35	31	62	64	1	49	53	56	32
25	35	51	5	10	38	22	22	53	13	21	46
19	47	20	20	26	18	47	26	18	55	41	9

#### 4.2.1 Positional Significance of Each Character in External Secret Key

The simulation parameters to analyze the positional significance in external secret key are the same as described in section 4.2. The analysis of master/primary key generation has been given in chapter 3. During the mapping process of the external secret key to some intermediate variables in proposed SBRS, the positional significance of the each character is retained. The sub-algorithm used for mapping external secret key to  $IC$ , is contained in the equations (4.1), (4.2), (4.3) and (4.4), which are given as:

$$K = K_1 K_2 K_3 \cdots K_{16} \quad (4.1)$$

$$IC_i = K_i / 256 \quad (4.2)$$

$$S = \sum_{i=1}^{16} RSGF_i^{K_i}(IC_i, p_i) \quad (4.3)$$

$$IC = S \bmod 1 \quad (4.4)$$

Equation (4.1) represents external secret key that consists of 16-characters. In equation (4.2), each character is uniformly mapped to a real number in the interval (0,1), that is represented by  $IC_i$  which serves as the initial condition for  $i^{th}$  RSGF. In equation (4.3),  $i^{th}$  RSGF with initial condition  $IC_i$ , is iterated  $K_i$  times to derive 16 random numbers that are summed together resulting in the intermediate variable  $S$ .

During the mapping process to the intermediate variable  $S$ , the positional significance of each character in the secret key is retained. From equation (4.2), it is evident that the  $i^{th}$  character in the secret key serves as initial condition for the  $i^{th}$  RSGF and RSGF is iterated  $K_i$  times, where  $K_i$  is the ASCII value of the corresponding  $i^{th}$

character. Hence different combinations of the secret key consisting of the same characters will result in different random numbers that are summed together, resulting in different values for the intermediate variable  $S$ . It can be seen from Table 4.4 converts  $S$  to a value between 0 and 1 and denoted by  $IC$ .

Table 4.4: ICs for Typical External Secret Keys

External Secret Key- $K$	$S$	$IC$
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'o' 'p'}	9.8458	0.8458
{'b' 'a' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'o' 'p'}	9.4438	0.4438
{'a' 'b' 'd' 'c' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'o' 'p'}	10.0774	0.0774
{'a' 'b' 'c' 'd' 'f' 'e' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'o' 'p'}	8.9865	0.9865
{'a' 'b' 'c' 'd' 'e' 'f' 'h' 'g' 'i' 'j' 'k' 'l' 'm' 'n' 'o' 'p'}	8.8735	0.8735
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'j' 'i' 'k' 'l' 'm' 'n' 'o' 'p'}	8.8053	0.8053
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'l' 'k' 'm' 'n' 'o' 'p'}	9.6060	0.6060
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'n' 'm' 'o' 'p'}	10.4678	0.4678
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'p' 'o'}	9.8739	0.8739
{'p' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'o' 'a'}	10.0333	0.0333
{'a' 'o' 'c' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'n' 'b' 'p'}	9.1932	0.1932
{'a' 'b' 'n' 'd' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'm' 'c' 'o' 'p'}	9.4743	0.4743
{'a' 'b' 'c' 'm' 'e' 'f' 'g' 'h' 'i' 'j' 'k' 'l' 'd' 'n' 'o' 'p'}	9.9999	0.9999
{'a' 'b' 'c' 'd' 'l' 'f' 'g' 'h' 'i' 'j' 'k' 'e' 'm' 'n' 'o' 'p'}	9.0108	0.0108
{'a' 'b' 'c' 'd' 'e' 'k' 'g' 'h' 'i' 'j' 'f' 'l' 'm' 'n' 'o' 'p'}	8.5547	0.5547
{'a' 'b' 'c' 'd' 'e' 'f' 'j' 'h' 'i' 'g' 'k' 'l' 'm' 'n' 'o' 'p'}	8.4095	0.4095
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'i' 'h' 'j' 'k' 'l' 'm' 'n' 'o' 'p'}	7.7317	0.7317
{'o' 'p' 'c' 'd' 'e' 'f' 'g' 'h' 'l' 'j' 'k' 'l' 'm' 'n' 'a' 'b'}	7.2468	0.2468
{'i' 'j' 'k' 'l' 'm' 'n' 'o' 'p' 'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h'}	6.7497	0.7497
{'e' 'f' 'g' 'h' 'm' 'n' 'o' 'p' 'a' 'b' 'c' 'd' 'l' 'j' 'k' 'l'}	8.2779	0.2779
{'a' 'b' 'c' 'd' 'l' 'j' 'k' 'l' 'e' 'f' 'g' 'h' 'm' 'n' 'o' 'p'}	8.68	0.68
{'m' 'n' 'o' 'p' 'i' 'j' 'k' 'l' 'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h'}	9.0319	0.0107
{'a' 'b' 'c' 'd' 'e' 'f' 'g' 'h' 'm' 'n' 'o' 'p' 'l' 'j' 'k' 'l'}	6.7246	0.8041
{'d' 'e' 'f' 'g' 'h' 'a' 'b' 'c' 'm' 'n' 'o' 'p' 'i' 'j' 'k' 'l'}	9.2388	0.1288
{'d' 'e' 'f' 'g' 'h' 'n' 'o' 'p' 'i' 'j' 'k' 'a' 'b' 'c' 'm' 'l'}	6.6594	0.4584
{'j' 'k' 'a' 'b' 'c' 'm' 'l' 'd' 'e' 'f' 'g' 'h' 'n' 'o' 'p' 'i'}	7.6044	0.7049
{'m' 'l' 'd' 'e' 'f' 'g' 'h' 'n' 'o' 'j' 'k' 'a' 'b' 'c' 'p' 'i'}	10.0153	0.0957
{'m' 'l' 'd' 'e' 'f' 'g' 'h' 'n' 'o' 'j' 'l' 'a' 'b' 'c' 'p' 'k'}	9.1755	0.9731
{'m' 'l' 'd' 'e' 'f' 'g' 'h' 'n' 'k' 'a' 'b' 'c' 'p' 'l' 'o' 'j'}	7.4701	0.5209
{'m' 'l' 'h' 'n' 'o' 'j' 'k' 'a' 'b' 'c' 'p' 'l' 'd' 'e' 'f' 'g'}	8.5193	0.6373



### 4.3 Effectiveness of SBR Interleaver as Security Device

#### 4.3.1 Traffic Analysis / Passive Eavesdropping

The security mechanism in the WLAN aims to achieve the security level comparable to that of the wired LANs. Due to the characteristics of the WLANs, the attacker can sniff and store all the traffic of WLAN. Hence it is very important to analyze whether the attacker may learn any meaningful information from the stored traffic of the WLAN. The attacker can try to manipulate confidentiality and integrity of WLAN as discussed in chapter 2.

To provide the security at the physical layers in the proposed SBR Interleaver scheme, each transmitting frame is encrypted/scrambled with unique key. In order to strengthen the security mechanism, master key/primary key is generated that will serve to initiate our proposed SBR Interleaver algorithm. The design of master key has been given in chapter 3. Let this primary key be  $IC_1$  that is used to encrypt/scramble the first frame. Let the frame to be scramble is denoted by  $F$ . It can be shown by:

$$S_1 = SBRI(F_1, IC_1) \quad (4.5)$$

where  $S_1$  is the first scrambled frame. To generate the new key to encrypt the second frame  $F_2$ , the next output of *RSNG* after scrambling the first frame serve as a key to encrypt  $F_2$  is  $IC_2$ . The remaining keys from  $IC_3$  to  $IC_N$  to encrypt the frames  $F_3$  to  $F_N$  respectively can be generated in the same way. The encrypted/scrambled frames  $S_2$  to  $S_N$  each with a unique key can be written as:

$$S_1 = SBRI(F_2, IC_2) \quad (4.6)$$

$$\vdots$$

$$S_1 = SBRI(F_N, IC_N) \quad (4.7)$$

where  $S_N$  is the total number of scrambled frames.

In our proposed SBR Interleaver each frame scrambled contain 64 symbols, so there are  $64!$  possible symbols combinations. We transmit 1000 random OFDM frames which lead to  $64000!$  or  $2^{64000}$  possible combinations. Hence it is infeasible to exhaustively search all the probable secret positions as each frame is encrypted/scrambled by the proposed SBR Interleaver with the different initial conditions. However when more than one frame is encrypted with the same initial conditions, the security of the proposed scheme will be low against the chosen plaintext attack which is evaluated later. From the above discussion, it is evident that encrypting each frame with the distinct initial condition makes it infeasible for the attacker to break the proposed SBR Interleaver through exhaustive searching technique.

The proposed SBR Interleaver helps to increase the entry barrier to break in, since it will take time and cost to break the key in real time. Moreover, attacker needs to check all possible combination which is infeasible in real time. Finally, and most importantly, our proposed SBR Interleaver used to scramble constellation symbol, and as shown earlier, with the wrong key the constellation symbol are still equally likely. So that, these scrambled constellation symbols entail no useful information to the attacker. After the transmission, only scrambled waveform is available which in fact entail no useful information. Moreover, it is really challenging to first extract correct bit level information from waveform then tries to manipulate mechanics used for WLAN.

In conclusion, proposed technique helps to prevent attacks on PHY layer and provide security by avoiding correctly recording and snooping MAC Protocol Data Unit (MPDU). Furthermore, PHY layer headers are also protected using SBRS. It contains Forward Error Correction (FEC), interleaving pattern, coding, phase offset etc. that are available for the receiver to obtain transmitted data. Encrypting PHY layer information further enhances the security of WLAN.



### 4.3.2 Data Forgery Attacks

The MAC address which is not encrypted, can serve as starting point to initialize different forgery attacks. The attacker eavesdrop the unprotected information and masquerades as access point (AP) to initialize de-authentication and disassociation attacks. The unprotected information available in MAC frame gives a chance for an attacker to sneak in and disrupts the transmission. The information in MAC header gives source and destination addresses controlling parameter and MAC address, which are there to determine correct destination. But, attacker uses this information and initializes session-hijacking attacks to disconnect devices. Typically an intruder forces a legitimate user to terminate its connection to an access point.

By snooping unprotected frames at MAC layer, intruder initializes Man-in-the-Middle attack to snoop their credentials by inserting himself between legitimate client and AP. By doing this the attacker forges the unprotected frames, modifies the frames and forwards it to the recipient. Intruder pretends to be authorized AP to client and authorized client to AP and fool them both. The details of data forgery attacks are given in chapter 2.

All these attacks are prevented by our proposed SBR Interleaver scheme. The unprotected frames at MAC layer and MAC header are protected so the data recorded at MAC layer is completely wrong, and wrong frame format does not give any information to intruder. For attacker, there is no information at all, since the transmitted data is encrypted at PHY layer. Data insertion attacks are also not possible because the data is encrypted and intruder needs to break the key to get the correct data. Intruder needs to check all possible key combination to get the correct key.

### 4.3.3 Denial of Service Attacks

One of the active attacks in WLAN is Denial of Service attacks (DoS). Typical DoS attacks involve flooding the network and preventing legitimate user to access the network resources. By using the characteristics of WLAN, attacker can launch DoS attack to disrupt the network traffic. At link layer, one type of attack is to forge the unprotected management frame to de-authenticate and disassociate frames to prevent the legitimate clients to use the network resources. The adversary forges the control



frame to initialize attack to disrupt the virtual carrier sense mechanism [J. Bellardo et al. 2003]. Hence the introduction of the SBR Interleaver at PHY layer secures such information which is left unprotected at link layer. The DoS attacks cannot be eliminated completely but can be minimized. Therefore, PHY layer security could help to prevent attacker to exploit the protocol weaknesses and resist against DoS attacks.

Since, PHY is secured with SBRs, so to initialize DoS attacks requires reasonable effort by attacker. With the proposed technique any insertion attack can be filtered out because it needs to break the key to get in. The worst de-authentication and disassociation attacks can be minimized and eliminated.

#### 4.4 Summary

In this chapter extensive analysis of SBR Interleaver as PHY layer security has been carried out. The analysis of SBR Interleaver is presented first using both chaotic and RAND function sequences and it is shown that proposed SBR Interleaver efficiently interleave input data elements with any random sequences. Additionally, proposed design does not depend on the random sequences that are used to initialize proposed SBR interleaver. First, the key sensitivity analysis is performed. It is shown that, small change in initial condition can generate completely different position vector, and recovering the data with wrong key produces nearly all position in error. Furthermore, it is shown that position elements generated with wrong key are also equally likely and it is not feasible to recover the data with wrong key. Moreover, the key sensitivity analysis gives nearly same results for both random sequences. The mapping of 128-bit key to master shows that the size of the key space is very large and generates random master keys each time. The detailed analysis of possible attacks on WLAN has been done. The traffic analysis/passive attacks can be prevented using proposed SBRs. All data at PHY layer is secured, because scrambling of constellation symbols leaves only waveform analysis for attacker and it takes time and cost to break in at bit level and mount attack. In addition, MAC header and frames are protected, which are the source for attacker to sneak in. Furthermore, unprotected information include coding, interleaving pattern and modulation scheme are all protected.

## Chapter

# 5

## Conclusion

In the previous chapters, we presented detailed background and literature review on various types of interleaver and in depth security analysis of wireless networks. Based on the knowledge that has been acquired from literature review and analysis of random interleavers along with its PHY layer security aspects for WLAN, we proposed a seed based random interleaver design and evaluated its performance under various conditions vis-à-vis other interleavers. In this chapter, we conclude the entire work that has been undertaken based on proposed SBR Interleaver.

### 5.1 Conclusion

In this thesis, the work that has been done is twofold. First, we analyze proposed seed based random (SBR) Interleaver based on performance parameter of spread, dispersion and BER as a function of length of burst error. Secondly, we study and analyze the suitability of proposed SBR Interleaver as a PHY layer security device. In a typical wireless communication system, interleaver is used along with channel coding to improve the performance of wireless communication system in burst noise introduced due to fading channels. An optimal interleaver must scatter a given burst of errors uniformly over a fixed block of data - a property that is measured by so called 'spread'. How randomly does an interleaver spread the given burst of errors every time is, however, measured by what is called 'dispersion'.



In this thesis, the idea is to use a pseudo-random sequence generator or logistic map based chaotic sequence generator together with a unique seed. The sequence range  $[0.1, 0.9]$  divided into equal sub-intervals of size equal to interleaver length. The unique property of our design is to avoid any repetition within these sub-intervals to design a unique scrambling matrix. The proposed scrambler as an interleaver gives rise to very good values of spread and dispersion. Moreover, proposed SBR Interleaver has near optimal properties of spread and dispersion. Our proposed interleaver spread the bits/symbols in such a way that 90% of input elements have average spread  $N/2$ . Further, the dispersion of proposed interleaver is in the range of 0.81-0.83. The proposed SBR Interleaver has been designed in such a way that the properties of spread and dispersion using both random sequences have almost same performance. Since our design is a seed based scrambler, the nature of input is irrelevant. Therefore, our interleaver can interleave either the bits or the symbols or the packets or even the frames.

Accordingly, the sub- objective is to also show that interleaving can change its position and introduce after the modulation. Thus, interleaving the bits before modulation or interleaving the symbols after modulation has the same advantage. However, interleaving post-modulation symbols requires smaller scrambling matrix size for  $M$ -ary modulations as compared to that that interleaves bits. The proposed interleaver is also used in an OFDM system. The performance results of pre- and post constellation mapper are obtained for an OFDM based worldwide interoperability for microwave access (WiMAX) system. At the end, a complete end-to-end IEEE 802.16d compliant fixed broadband wireless access (FBWA) system, an early model of WiMAX system, is developed in MATLAB-SIMULINK.

Our proposed Interleaver is compared with MATLAB<sup>®</sup> random interleaver to analyze the performance in correcting the length of burst errors that are introduced manually. Our proposed interleaver efficiently works in burst error environment and converts maximum number of burst errors into single errors as compared to MATLAB<sup>®</sup> random interleaver.

There is also a side advantage of this seed based interleaver, in that it generates a variety of unique random-looking interleaving sequences. Only a receiver that has the



knowledge of the input seed can generate this sequence and no one else. If the interleaving patterns are kept secure then it can possibly be used to introduce an extra layer of security at physical (PHY) layer. An added motivation is to analyze the security implications of the proposed interleaver. The proposed SBR Interleaver is also analyzed for its suitability to secure PHY layer security. In wireless network, previously, the MAC frames that contain source and destination information and all other management and control information and the security of these frames are compromised. These frames are tending to use to facilitate wireless traffic but eavesdropper utilizes these frames to initialize number of attacks. The proposed SBR Interleaver prevents all attacks on the robustness of WLAN. At PHY layer, coding, interleaving and modulation patterns are not protected. These known patterns are used to facilitate the receiver to successfully synchronize and to restore the transmitted data. Since the scrambling is done after the constellation symbols, all the information at PHY layer is protected. The only information for the attacker is the waveform which is also equally likely as the original waveform. In order to recover the key, attacker needs to first recovered interleaving sequences then at bit level tries to break the mechanics of confidentiality and integrity. Our proposed technique increases the entry barrier to break in by introducing a level of security at PHY layer. In order to analyze the strength of the SBR Interleaver, key sensitivity analysis is carried out.

## 5.2 Contribution of this Research Work

- A novel design of seed based random interleaver with sequence generated from two random sources: chaotic sequence using chaotic logistic map and MATLAB RAND function.
- It is also shown that the spread and dispersion of both CLM based SBR Interleaver and RAND based SBR Interleaver is quite same.
- Our study reveals that interleaver can change its position and can be introduced at post modulation level. The comparison of pre- and post modulation interleaver is carried out to compare the performance both at pre- and post modulation levels in terms of complexity and interleaving properties of dispersion and spread.

- The proposed scheme is analyzed, for burst error correction capability, and compared with MATLAB random interleaver. Our proposed design efficiently converts larger number of burst errors into simple errors as compared to MATLAB random interleaver.
- The proposed interleaver is also analyzed in an OFDM system. At the end, a WiMAX model compliant with IEEE802.16d is developed and the interleaver block is introduced at both pre- and post constellation mapper block. The performance of the said interleaver is compared.
- Finally, proposed seed based random interleaver is exploited at PHY layer to analyze its suitability as a PHY layer security device. The key-sensitivity is carried out and the effectiveness of proposed interleaver against brute force and various data forgery attacks are discussed.

### 5.3 Suggested Future Work

- Proposed seed based random interleaver is basically a random scrambling, and the mapping is based on S- box. The influence of advance encryption standard (AES) S- box in designing scrambler has to be adequately analyzed.
- The performance comparison of AES S- box with proposed design has to be adequately analyzed.
- Issues relating to implementation of proposed SBR Interleaver on chips and its cost analysis also have to be adequately analyzed. The specification of hardware and the way it affect the performance of communication system need to be examined in detail.
- Also, the implementation of proposed SBR Interleaver design as a PHY layer device and its cost analysis also have to be adequately analyzed.

- Further, use this design to multiuser scenario like orthogonal frequency division multiple access (OFDMA). The required modification in the proposed system for successful implementation need be adequately analyzed.
- The implementation of proposed interleaver in applications like turbo codes need to be developed to adequately analyze the performance. This will further help to explore the performance of proposed design.



## PUBLICATIONS

### (Published papers)

1. Muhammad Asif Khan, M. Asim, Varun Jeoti and Shahid Manzoor “*On Secure OFDM system: Chaos Based Constellation Scrambling*”, IEEE International Conference on Intelligent & Advanced System (ICIAS). PP: 484-488, 2007. Kuala Lumpur, Malaysia.
2. Muhammad Asif Khan, M, Asim, Varun Jeoti, Shahid Manzoor “*Chaos Based PHY Layer Security for OFDM system*”, National Postgraduate Conference 2008, Universiti Teknologi PETRONAS, Malaysia
3. Muhammad Asif Khan, M. Asim, Varun Jeoti, Shahid Manzoor “*Chaos Based constellation scrambling for OFDM system: Security & Interleaving Issues*”, IEEE international symposium on information technology (ITSIM), vol 4, pp: 2479-2485, 2008. Kuala Lumpur, Malaysia
4. Muhammad Asif Khan, M. Asim, Varun Jeoti, Shahid Manzoor “*A Chaos Based Random Interleaver Design and Its Analysis*”, IEEE Regional Student conference on Research and Development (SCOREd) 2008, Johor Bahru, Malaysia

### (Submitted papers)

1. M. Asif Khan, M. Asim, V. Jeoti and S. Manzoor “*Secure Interleaving: PHY layer Security Enhancement of OFDM Based System*” 7<sup>th</sup> Annual IEEE Consumer Communication and Network Conference (CCNC) 2009. Nevada, USA
2. M. Asif Khan, M. Asim, V. Jeoti and S. Manzoor “*A Novel Seed Based Post Modulation Interleaver : Design and Analysis* ” IEEE international conference on signal and image processing Applications 2009 (ICSIPA 2009), Kuala Lumpur, Malaysia

## JOURNAL PUBLICATIONS (Under Preparation)

1. Muhammad Asif Khan, Varun Jeoti and Shahid Manzoor. “*A Novel Seed Based Random Interleaver Design and Its Analysis*”. Manuscript under preparation for Electronics and Telecommunication Institute (ETRI) Journal
2. Muhammad Asif Khan, Varun Jeoti and Shahid Manzoor. “*Analysis of Pre- and Post Modulation Interleaver and Its Security Aspects*”. Manuscript under preparation for Electronics and Telecommunication Institute (ETRI) Journal

## REFERENCES

- [A. B. James et al. 2004] An analysis of interleaver for robust speech recognition in burst-like packet loss. *IEEE International conference on acoustic speech and signal processing (ICASSP)*, 2004.
- [A. Goldsmith et. al. 2005] Wireless Communications. *Cambridge University Press*, 2005
- [A. Martinaz et al. 2008] Beacon frame spoofing attack detection in IEEE 802.11 network. *In the proceeding of third international conference on availability Reliability and Security*, 2008.
- [A. Pal et al. 2006] Method and apparatus for a security system for wireless networks. USA patent publication, pub no. US 2006/ 0126841 A1, 15<sup>th</sup> June, 2006.
- [A. Stubblefield et al. 2002] Using the Fluhrer, Mantin, and Shamir attack to break WEP. *In the proceeding of Network and Distributed Systems Symposium*, February 2002.
- [B. Aboba et al. 1999] PPP EAP TLS authentication protocol. *RFC 2716*, October 1999.
- [B. Schneier et al. 1996] Applied Cryptography: Protocols, Algorithms, and Source Code in C. *John Wiley and Sons, New York, second edition*, 1996.
- [B. Sklar et al.1998] Digital communications fundamentals and applications. *Prentice-hall publications*, ISBN. 0- 1- 212713- X, 1988
- [C. A. Leon et al. 2004] Analysis of dispersion and spread properties of interleaver for turbo codes. *Computer research conference*, April 2004
- [C. Berrou et al. 1993] Near Shannon limit error-correcting coding and decoding : turbo-codes. *In the Proceedings of ICC'93*, Geneva, pp. 1064-1070, May 1993.
- [C. He et al. 2004] Analysis of 4- way handshake. *In Proceedings of the Third ACM International Workshop on Wireless Security*, WISE 2004.



- [C. He et al. 2004] Analysis of the 802.11 4- way handshake. *In proceeding of Wise 2004*
- [C. He et al. 2005] Security analysis and improvements for IEEE 802.11i. *The 12th Annual Network and Distributed System Security Symposium (NDSS'05)*, pages 90-110. Feb. 2005
- [C. Heegard et al 1999] Turbo Coding. *Boston: Kluwer Academic Publishers*, pp:54-55, 1999.
- [C. J. C. Bravo et al 2004] Algebraic construction of interleaver using permutation polynomials. *IEEE international conference on communications (ICC)*, June 2004
- [C. J. C. Bravo et al. 2003] Permutation polynomials for interleavers in turbo codes. *In the Proceeding of IEEE International Symposium of Information Theory (ISIT'03)*, pp. 318, Yokohama, Japan, Jul. 2003.
- [C. L. Shuba et al. 1997] Analysis of Denial of Service Attacks on TCP. *In proceeding of IEEE symposium on security and privacy*, pp: 208- 223. 1997.
- [C. Liu et al. 2007] A Solution to WLAN's authentication and association attacks. *IAENG international journal of computer science (IJCS)*, Nov 2007
- [C. Liu et al. 2008] Rouge access point based attacks against 802.11 WLAN's. *In proceeding of fourth advanced international conference on telecommunications*, 2008.
- [C. Rigney et al. 2000] Remote Authentication Dial In User Service (RADIUS). *RFC 2865*, June 2000.
- [Cisco System, 2002] Cisco Aironet response to University of Maryland's paper. *An initial security analysis of the IEEE 802.1X standard*, August 2002
- [D. Chen et al. 2003] Protecting wireless networks against a Denial of Service attack based on virtual jamming. *In Poster Session of MobiCom2003*, September 2003



- [D. Divsalar et al. 1995] Turbo codes for PCS applications. In *Proceeding of IEEE International Conference on Communications (ICC'95)*, vol. 1, pp. 54-59, Seattle, June 1995.
- [D. Dzung et al. 2005] Data encryption on the physical layer of a data transmission. USA patent publication, pub no. US 2005/ 0055546 A1, 2005.
- [D. Whiting et al. 2003] Counter with CBC-MAC (CCM). *RFC 3610*, September 2003.
- [F. Daneshgaran et al. 2004] Interleaver pruning for the construction of variable length turbo codes. *IEEE Transactions on Information Theory*, Vol. 50, No. 3, pp.455-467, March 2004
- [F. Zhang et al. 2005] Security proof of a 4- way handshake protocol in IEEE 802.11i. *Lecture notes in computer science, springer berlin*, vol 3805/2005. 2005.
- [G. D Forney et al. 1971] Burst-correcting codes for the classic bursty channel. *IEEE Transaction on Communication Technology*, vol. COM-19, pp. 772-781, Oct. 1971.
- [H. Cheung et al. 2005] FBI Teaches Lesson in how to break into Wi-Fi networks, 2005. <http://informationweek.networkingpipeline.com/160700382>.
- [H. Hove et al. 1982] Error correction in the compact disc system. *Phillips Technical Review*, Vol. 40, No. 6, 1982.
- [H. Imai et. al. 1977] A new multilevel coding method using error-correcting codes. *IEEE Transactions on Information Theory*, vol. IT-23, pp. 371-377, Sep. 1977.
- [H. R. Sadjadpour et al. 2001] Interleaver design for turbo codes. *IEEE Journal on Selected Areas in Communications*, vol. 19, no. 5, pp. 831-837, May 2001.
- [I. S. Reed et al. 1960] Polynomial codes over certain finite fields. *SIAMJ Applied Mathematics*, vol. 8, pp. 300-304, June 1960.
- [IEEE 802.11, 1999] IEEE Standard 802.11-1999. Information technology - Telecommunications and information exchange between systems - local and metropolitan

area networks - specific requirements - Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications, 1999.

[**IEEE 802.1X. 2001**] IEEE standard for local and metropolitan area networks - port-based network access control, June 2001.

[**IEEE P802.11i/ D10.0. 2004**] IEEE P802.11i/D10.0. Medium Access Control (MAC) security enhancements, amendment 6 to IEEE standard for Information technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications, April 2004.

[**J. Bellardo et al. 2003**] 802.11 Denial-of-Service attacks: real vulnerabilities and practical solutions. *In the USENIX Security Symposium*, pages 15–28, August 2003.

[**J. Bellardo et al. 2004**] 802.11 Denial-of-Service attacks: real vulnerabilities and practical solutions. *In the USENIX Security Symposium*, pages 15–28, August 2003.

[**J. Krovjak et al. 2006**] Analysis, demand, and properties of pseudorandom number generator. *mukulasska kryptobesidk*, ISBN 80- 903083- 7- 6, PP: 55- 56. 2006.

[**J. L. Ramsay et al. 1970**] Realization of optimum interleavers. *IEEE Transactions on Information Theory*, vol. IT-16, no. 3, May 1970.

[**J. Li et al. 2002**] Low -complexity, capacity-approaching coding schemes: design, analysis and applications. *Ph.D Dissertation*, pp: 58, *Texas A & M University* , Dec 2002.

[**J. R. Walker et al. 2000**] Unsafe at any key size; an analysis of the WEP encapsulation. *IEEE Document 802.11-00/362*, October 2000.

[**J. S. Park et al. 2004**] WLAN security: current and future. *IEEE Internet Computing*, vol. 8, no.2, pp. 76–83, April 2004.

[**K. Andrews et al. 1997**] A Theory of Interleavers. *Technical Report, UMI Order Number: TR97-1634*., Cornell University. 1997.



- [K. S. Andrews et al. 1998] Interleaver design methods for turbo codes. *In the Proceeding of IEEE International Symposium on Information Theory (ISIT'98)*, Cambridge, MA, August 1998.
- [K. Xie et al. 2006] On the analysis and design of good algebraic interleaver. proceeding of 4<sup>th</sup> international symposium on turbo codes and related topics, Munich, Germany 2006.
- [L. Blunk et al. 2003] Extensible Authentication Protocol (EAP). *Internet Draft draft-ietf-eap-rfc2284bis-06.txt*, September 29 2003.
- [L. Dinoi et al. 2003] Design of prunable S- random interleaver. 3<sup>rd</sup> *International symposium on turbo codes and related topics*, Brest, France. 2003.
- [L. dinoi et al. 2005] Design of fast pruable S- random interleaver. *IEEE transaction on wireless communications*, vol 5, no 5, Nov 2005.
- [L. Trifina et al. 2007] Increasing  $S$  parameter of an interleaver. *International symposium on signal circuit & systems (ISSCS)*, 2007.
- [M. Eroz et al. 1999] On the design of prunable interleavers for turbo codes, 49<sup>th</sup> *IEEE conference on vehicular technology*, 1999.
- [M. Drieberg 2005] MIMO channel estimation for applications in fixed broadband wireless access system, *Master dissertation*, pp:63-68, *Universiti Teknologi PETRONAS*, 2005.
- [M. Malekzadeh et al. 2007] Security improvement for management frames in IEEE 802.11 wireless networks. *International Journal of Computer Science and Network Security (IJCSNS)*, vol.7, no. 6, June 2007
- [N. Asokan et al. 2002] Man-in-the-Middle in tunneled authentication protocols. *Technical Report 2002/163*, October 2002.



[N. Brisov et al. 2001] Intercepting mobile communications: the insecurity of 802.11. *In the 7th Annual International Conference on Mobile Computing and Networking*, July 2001.

[N. Cam-Winget et al 2003] Security flaws in 802.11 data link protocols. *SPECIAL ISSUE: Wireless networking security, Communications of the ACM*, 46(5):35–39, May 2003.

[NIST. 2001] National Institute of Standards and Technology, FIPS Pub 197: Advanced Encryption Standard (AES), November 26 2001.

[O. Y Takeshita et al. 2006] On maximum contention-free interleavers and permutation polynomials over integer rings. *IEEE transaction on information theory*, vol.52, issue.3, pp. 1249-1253, March 2006

[O. Y. Takeshita et al. 2000] New deterministic interleaver designs for turbo codes. *IEEE Transactions on Information Theory*, vol.46, no.6, pp: 1988-2006, Sept. 2000

[P. Elias et al. 1960] Coding for practical communications systems. *Presented at the URSI 13th General Assembly*, London, 1960

[P. Popovski et al. 2004] Design of flexible-length S-random interleaver for turbo codes. *IEEE communication letter*, vol 8, no 7, July 2004.

[P. Shibly et al. 2001] Open WLANs: the early result of Wardriving, 2001.

[Q. Ling et al. 2004] Physical layer built-in security enhancement of DS-CDMA systems using secure block interleaving. *IEEE thirty-eight asilomar conference on signals, systems and computers*, vol. 1, issue 7, pp: 1105- 1109, 10<sup>th</sup> Nov 2004.

[Q. Ling et al. 2005] Physical layer built in security enhancement of DS-CDMA system using block interleaving. *Publication in the IEEE globecom proceeding*, 2005

[R. canetti et al. 2002] Universally Composable Notions of Key Exchange and Secure Channels. *In proceedings of Eurocrypt*, 2002

[R. Garelo et al. 2001] Interleaving properties and their application to the trellis complexity analysis of turbo codes. *IEEE Transactions on communications*, Vol.49, No. 5, May 2001.

[S. Dolinar et al. 1995] Weight distribution of turbo codes using non random and random permutation. JPL *progress report 42-122*, 1995

[S. fluhrer et al 2001] Weaknesses in the key scheduling algorithm of RC4. *Lecture Notes In Computer Science, Revised Paper from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages1–24, 2001.

[S. N. Crozier et al. 1999] Performance of turbo codes with relative prime and golden interleaving strategies. *In the Proceeding of the 6th International Mobile Satellite Conference (IMSC'99)*, Ottawa, Ontario, pp. 268-275, June 1999.

[V. Moen et al 2004] Weakness in the Temporal Key Hash of WPA. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8(2):76–83, April 2004.

[V. Erceg et. al. 2003] Channel Models for Fixed Wireless Applications. *IEEE802.16a-03/01*. New York: The Institute of Electrical and Electronics Engineers Inc.

[W. A. Arbaugh et al. 2001(I)] An inductive chosen plaintext attack against WEP/WEP2. Presentations to IEEE 802.11 TG1, May 2001.

[W. A. Arbaugh et al. 2001(II)] Your 802.11 network has no clothes. *In the first IEEE International Conference on Wireless LANs and Home Networks*, pp 131–144, December 2001.

[W. feng et al. 2002] A Code-Matched Interleaver Design for Turbo Codes. *IEEE Transactions on Communications*, Vol. 10 50, No. 6, pp. 926-937, June 2002,

[Y. B Luis et al 2004] Properties of a class of permutations over finite fields and turbo codes. *PRISM*. 2004.

[Y. Hwang et al. 2004] Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design. IEEE Transaction on signal processing, vol. 52, issue. 9, 2004.